7º CENTRO TELEMÁTICA ÁREA- CONTROLE DE CUSTOS

Estudo Técnico Preliminar 14/2026

1. Informações Básicas

Número do processo: 64195.001002/2026-14

2. Introdução

2.1. O 7º Centro de Telemática de Área (7º CTA) é a Organização Militar (OM) do Exército Brasileiro responsável por prover, no âmbito estratégico do Comando Militar do Planalto (CMP) e Quartel General do Exército, os serviços essenciais ao Sistema de Telemática do Exército (SISTEx). Sua missão principal consiste em assegurar conectividade segura, resiliente e de alta disponibilidade entre as organizações militares do Exército, por meio da implantação, operação e sustentação de soluções tecnológicas avançadas, abrangendo tanto a infraestrutura física quanto a lógica.

2.2. Nesse contexto, o 7º CTA desempenha papel fundamental na integração das redes de comunicação, na implementação de mecanismos de segurança cibernética e na manutenção da conectividade em tempo real, contribuindo para a continuidade e a confiabilidade das operações militares. Além disso, atua no apoio à coordenação interinstitucional e à integração com sistemas civis, ampliando a capacidade de interoperabilidade e garantindo o funcionamento dos serviços críticos mesmo em ambientes adversos.

2.3. Para assegurar a conectividade e a hospedagem dos sistemas corporativos do Exército Brasileiro, o 7º CTA dispõe de uma rede metropolitana e de um ambiente de *Data Center* de alta disponibilidade, denominado *Data Center* Principal do Exército Brasileiro (*Data Center* Coronel Ricardo Franco), localizado em Brasília-DF. Contudo, embora estratégico e essencial ao funcionamento da Força, esse ambiente apresenta limitações de capacidade diante da crescente demanda por processamento, armazenamento e suporte a novas cargas computacionais.

2.4. Nesse cenário, o presente estudo tem por finalidade analisar a viabilidade técnica e econômica da expansão da capacidade do *Data Center* Coronel Ricardo Franco, de modo a ampliar sua aptidão para hospedar os sistemas do Exército Brasileiro, com especial atenção à incorporação de recursos de processamento voltados à Inteligência Artificial (IA).

2.5. Atualmente, o *data center* operado pelo 7º CTA não dispõe de capacidade computacional plenamente compatível com o crescimento do volume, da complexidade e dos requisitos de desempenho dos sistemas modernos, muitos dos quais já incorporam ou demandam funcionalidades baseadas em Inteligência Artificial. Essa tendência se manifesta em diversas áreas, como operações militares, vigilância, monitoramento, sistemas hospitalares, defesa cibernética, logística, ensino, gestão, comando e controle, entre outras. Nesses contextos, o uso de IA tende a elevar a eficiência operacional, reduzir o tempo de resposta, qualificar a análise situacional e ampliar a capacidade de prevenção e mitigação de riscos, tanto na esfera administrativa quanto na operacional.

2.6. Diante desse panorama, a implantação de um data *data center* voltado para IA, em ambiente próprio e controlado pelo Exército, apresenta-se como medida estratégica para assegurar soberania tecnológica, proteção da informação e autonomia operacional. A dependência exclusiva de serviços de IA de mercado (especialmente em nuvem pública) pode impor limitações críticas, como exposição de dados, restrições tecnológicas, condicionantes legais, auditoria e rastreabilidade.

2.7. Além disso, um *data center* especializado para IA permite padronizar e escalar capacidades computacionais, concentrando recursos (GPU, armazenamento de alto IOPS e ferramentas MLOps) de modo racionalizar investimentos e acelerar o ciclo de desenvolvimento e implantação de modelos de IA, atualmente em estudos pelo Centro de Desenvolvimento de Sistemas (CDS). Tal infraestrutura também favorece a formação e retenção de

competências internas, a realização de pesquisas aplicadas e a integração com sistemas corporativos já existentes, garantindo uma melhor governança de TIC do Exército.

2.8. Assim, este Estudo Técnico Preliminar busca caracterizar a necessidade, os requisitos e as alternativas para viabilizar a implantação de uma infraestrutura de *data center* orientada a IA, alinhada às demandas atuais e futuras do Exército Brasileiro, com foco em segurança, disponibilidade, desempenho, escalabilidade e eficiência ao longo do ciclo de vida da solução.

2.9. Este estudo é baseado em uma demanda do Departamento de Ciência e Tecnologia (DCT) do Exército (Órgão de Direção Setorial do Exército Brasileiro) conseguinte da necessidade de garantir o acompanhamento tecnológico e garantir a soberania das informações sensíveis, não dependendo de soluções de mercado.

2.10. A implantação de um *data center* de IA no Exército Brasileiro é respaldada por diversos documentos normativos que embasam essa decisão estratégica. No contexto do Ministério da Defesa e do Exército Brasileiro há um arcabouço normativo abrangente, gerencial e de planejamento estratégico, que estabelece as diretrizes fundamentais para a Defesa Nacional e para as atividades de Tecnologia da Informação e Comunicação (TIC) no âmbito do Exército.

2.11. Um investimento nessa infraestrutura está em conformidade com as diretrizes estabelecidas em tais documentos, demonstrando o compromisso do Exército Brasileiro em fortalecer sua capacidade de resposta e defesa do país. A Diretriz Estratégica de Inteligência Artificial para o Exército Brasileiro (Portaria – EME/C Ex nº 1.318, de 14 de maio de 2024) estabelece, por exemplo, o balizamento normativo para a implementação e o emprego da IA na Força, sendo um documento fundamental para a especificação técnica de infraestruturas de processamento de dados.

2.12. Nesse contexto, cabe ressaltar que o atual ambiente do *Data Center* Ricardo Franco foi projetado com áreas técnicas capazes de incorporar uma expansão de equipamentos e capacidades, podendo assim absorver a atual demanda sem necessidade de alterações estruturais ou novas edificações. Contudo, é importante observar que nesse novo cenário, um volume maior de processamento será demandado, impondo uma densidade de potência elevada, o que pode resultar em mudanças de solução principalmente em relação ao sistema de resfriamento.

3. Descrição da necessidade

3.1. Fundamentação:

3.1.1. O Exército Brasileiro (EB), por intermédio do Estado-Maior Exército, instituiu, com base na publicação da Portaria – EME/C Ex nº 1.535, DE 23 de maio de 2025, grupo de trabalho para a estruturação da Governança e da Gestão da Inteligência Artificial no Exército Brasileiro, grupo esse que vem estabelecendo prioridades e definindo diretrizes de emprego de soluções.

3.1.2. Nesse contexto, em trabalho recente (Emprego da Inteligência Artificial no Exército Brasileiro - PI-CPAEx 2025), publicado pelo Curso de Política, Estratégia e Alta Administração do Exército ao Alto Comando da Força, ficou evidenciada a **necessidade de se considerar a questão da infraestrutura (*data center*)** e da segurança cibernética, como elemento estruturante nos projetos de aplicações em IA, sob o **risco** da atual infraestrutura **não** suportar o aumento da demanda por recursos de IA.

3.1.3. Além disso, na última Reunião do Alto Comando do Exército (RACE) de 2025, foi orientado que todos os projetos estratégicos do Exército avaliassem a possibilidade de inclusão da IA em seus escopos, o que tende a demandar um aumento por consumo de recursos computacionais.

3.1.4. Em razão da legislação vigente (Lei Geral de Proteção de Dados - Lei nº 13.709/ 2018, a Instrução Normativa SGD/ME nº 94/ 2022, da Instrução Normativa GSI/PR nº 5/ 2021, da Política Nacional de Defesa - PND e Estratégia Nacional de Defesa - END, aprovada pelo Decreto nº 12.725, de 18 de novembro de 2025, da Diretriz Estratégica de Inteligência Artificial para o Exército Brasileiro, aprovada pela Portaria - EME/C Ex nº 1.318, de 14 de maio de 2024, e da Diretriz para a Contratação e o Uso Seguro de Serviços de Computação em Nuvem no Âmbito do Exército Brasileiro, aprovada pela Portaria - EME/C Ex nº 1.535, de 4 de novembro de 2025), dos dados tratados e das informações processadas, é imprescindível que o EB tenha autonomia dos

dados sob sua responsabilidade, garantindo a Soberania dos Dados; desse pressuposto, demanda-se grande investimento em TI para a adoção de uma nuvem privada, inclusive para processamento de IA, e para consolidação dos dados estratégicos.

3.1.5. Para operacionalizar a TI de todo o Exército Brasileiro, foi definido o Sistema de Telemática do Exército (SisTEx), que:

3.1.5.1. Tem por finalidade proporcionar as comunicações estratégicas, interligando as bases física e lógica do SEC²Ex e realizando a integração com os demais sistemas utilizados pelo SC²Ex;

3.1.5.2. Permite o transporte, processamento e armazenamento de dados, bem como o tráfego de voz, essenciais para o Exército planejar, dirigir e controlar suas ações, em todos os níveis da estrutura organizacional, desde o mais alto nível, com segurança; e

3.1.5.3. É composto pelo seu Órgão Central, o Centro Integrado de Telemática do Exército (CITEx), e Elementos Operacionais – Organizações Militares Diretamente Subordinadas (OMDS) –, os Centros de Telemática de Área (CTA) e os os Centros de Telemática (CT).

3.1.6. Ademais, com foco e alinhamento para a contratação em alusão, cabe reforçar algumas atribuições do SisTEx, destacados em itens do arcabouço a seguir, onde constam especificamente:

3.1.6.1. Na Diretriz Estratégica de Tecnologia da Informação do Exército (EB10-D-01.037), aprovada pela Portaria - EME/C Ex nº 1.326, de 29 de maio de 2024, aponta como atribuição do CITEx como órgão gestor, migrar a hospedagem dos sistemas críticos e corporativos do EB para o CITEx, ou para as suas OMDS, quando aplicável, alinhado ao OETI 1 e 4;

3.1.6.2. Na Diretriz Organizadora do Sistema Estratégico de Comando e Controle do Exército (EB20-D-02.037), aprovada pela Portaria EME/C Ex nº 1.389, de 21 de agosto de 2024, que o SisTEx fornece ou hospeda, entre outros, *Data Centers* Corporativos do Exército, alinhado ao OETI 1 e 4; e

3.1.6.3. No PETI 2024 - 2027, Plano Estratégico de Tecnologia da Informação (PETI) do Exército Brasileiro (EB10-P01.005) 2024-2027, aprovada pela Portaria - C Ex nº 2.506, de 14 de julho de 2025, implantar a aplicação de IA em C2 e Informação, sob responsabilidade do DCT - organização que enquadra o CITEx e o 7º CTA -, a fim de promover a transformação digital aliada à segurança cibernética no Exército (OETI 4).

3.1.7. Diante da estratégia em curso, a presente contratação justifica-se pela necessidade em garantir, ao *Data Center* Ricardo Franco, e em última análise ao Exército, capacidade de hospedagem de equipamentos de alta densidade e capacidade para sustentar sistemas corporativos do Exército Brasileiro suportados ou que entregam capacidade de IA.

Alinhamento com a Política de Inteligência Artificial de Defesa

3.1.8. A necessidade de ampliação e modernização da infraestrutura do datacenter deve ser considerada também sob a perspectiva das novas demandas institucionais relacionadas ao processamento intensivo de dados, à adoção de soluções avançadas de tecnologia da informação e ao desenvolvimento de capacidades de Inteligência Artificial no âmbito da Defesa.

3.1.9. Nesse contexto, a **Portaria GM-MD nº 4.360, de 24 de agosto de 2026**, que aprova a Política de Inteligência Artificial de Defesa, estabelece, entre seus objetivos, o desenvolvimento de capacidades de Inteligência Artificial para a Defesa Nacional e, expressamente, a **implantação das estruturas necessárias à Inteligência Artificial de Defesa**, bem como da correspondente governança e gestão.

3.1.10. Dessa forma, a ampliação da infraestrutura de datacenter encontra-se alinhada à necessidade de prover uma base tecnológica capaz de suportar, de forma segura, resiliente, escalável e contínua, as atuais e futuras demandas computacionais da Força, inclusive aquelas associadas à utilização de sistemas de Inteligência Artificial, processamento de grandes volumes de dados e cargas computacionais de elevada densidade.

3.2. Cenário Atual:

3.2.1. Atualmente, o Sistema *Data Centers* Corporativos (SisDC) do Exército Brasileiro possui 2 (dois) *Data Centers* (DC) próprios certificados: o *Data Center* Ricardo Franco (DC RF), instalado e operado em Brasília-DF, inaugurado em 2018, sob a gestão do 7º Centro de Telemática de Área (7º CTA), e o *Data Center* Marechal Rondon (DC MR), instalado e operado em São Paulo-SP, inaugurado em 2025, sob a gestão do 3º Centro de Telemática de Área (3º CTA).

3.2.2. Esses DC, considerados estratégicos para a manutenção e constante aperfeiçoamento da capacidade de Comando e Controle da Força, hospedam as principais soluções de TI do Exército, com destaque para os principais Sistemas Corporativos, Base de Dados Corporativa, Serviço de Correio Eletrônico, Rede Privada Segura (VPN), dentre outras.

3.2.3. O advento da Inteligência Artificial (IA) impõe desafios infraestruturais ao SisDC, dado que o *hardware* especializado de IA, com GPUs H200 ou B200, exige uma densidade energética até 5 (cinco) vezes superior à dos servidores convencionais. Nesse contexto, a adaptação de DC projetados para *hardware* de TI tradicionais exige a atuação técnica especializada para implantação e integração da infraestrutura necessária para receber uma grande quantidade de *hardware* de IA, com a necessidade de reestruturação complexa, envolvendo o redimensionamento de GMG e dos quadros de distribuição elétrica, a implementação de sistemas de redundância de energia (UPS) de alta densidade e o projeto de soluções avançadas de climatização.

3.2.4. Para iniciar a contextualização sobre o DC RF, cabe destacar:

3.2.4.1. Os equipamentos da sua infraestrutura são de 2017, embora o DC tenha sido inaugurado em 2018;

3.2.4.2. Possui certificações TIER III Uptime Institute em *Design* e *Facilities* (da mesma forma que o DC MR);

3.2.4.3. Hospeda 6 (seis) Servidores de IA, totalizando 12 (doze) Unidades de Processamento Gráfico (GPU), especificados pelo CITEx, cuja gestão é de responsabilidade do Centro de Desenvolvimento de Sistemas (CDS) do Exército;

3.2.4.4. Tem condições de absorver uma capacidade elétrica e a equivalente de dissipação térmica de **até o limite de 140 kVA**, para todas as demandas do Exército, sejam elas de IA ou não; com isso, a capacidade de absorver soluções de IA está limitada a esse valor sem a necessidade de intervenções de infraestrutura elétrica ou de climatização (*retrofit*).

3.2.5. Com base no item 3.2.1. e 3.2.4, demostra-se o conhecimento técnico do CITEx e de suas OMDS na implantação de *data centers*, aquisição de equipamentos de IA e respectiva hospedagem.

3.2.6. Adicionalmente, a fim de estabelecer um prognóstico, lista-se as recentes solicitações e ações em curso:

3.2.6.1. Há tratativas em andamento com o Centro Gestor Operacional do Sistema de Proteção da Amazônia (CENSIPAM) do MD para a instalação de um supercomputador (HPE Cray XD690, com 8 GPUs B300 SXM, de 10 unidades de rack padrão de 44 U) no DC RF ainda no corrente ano (além de outros equipamentos de TI), com emprego de recursos de IA em proveito daquele órgão. Esse supercomputador, dado sua grande capacidade, demandará uma elevada carga energética da ordem de **30 kVA**; e

3.2.6.2. Hospedagem no DC RF visando processamento de aprendizagem de cargas de trabalho de IA para suportar o EBOT, cujo *hardware* estimado necessário para esse ChatBot, considerando arquiteturas de referência para modelos LLM de grande porte (70B a 405B parâmetros) e soluções de mercado (ex: Cisco AI POD), onde se destaca uma demanda nominal de pico na ordem de **50 kVA** em apenas três servidores.

Categoria	Item / Especificação Técnica	Quantidade
Processamento	**GPU NVIDIA H200** (141GB HBM3e - SXM5)	24 (8 por nó)
Memória Host	Memória RAM DDR5 4800MHz	3.072 GB
Armazenamento	Storage All-Flash NVMe (Escrita Paralela)	100 TB
Rede de IA	Switches e Placas InfiniBand (400Gbps)	Conjunto
Servidores	**Nós de Computação** (ex: UCS p/ 8 GPUs cada)	03 unidades
Energia	Consumo de Pico Estimado	52,63 kVA
Peso	Peso Total Estimado do Rack	~650 kg

3.2.7. Conclui-se até aqui que, para as necessidades apresentadas, que o SisDC precisaria ofertar recursos computacionais equivalente na ordem de 50 GPUs para suportar as demandas atuais do Exército Brasileiro em processamento massivo de IA.

3.2.8. Logo, as principais limitações do SisDC incluem:

3.2.8.1. Ausência de *hardware* de alta capacidade (GPU) necessário para modelos de IA Generativa (LLM); e

3.2.8.2. Capacidade reduzida para hospedagem de Soluções de Infraestrutura de IA (SIIA), como servidores e demais periféricos desse ecossistema, sendo imprescindível adequação completa dos ambientes de hospedagem do DC RF para sustentar processamento de IA.

3.3. Prospecções iniciais:

3.3.1. Dada a motivação e diante de todo esse cenário, o CITEx, organização que enquadra o 7º CTA, conduziu, conforme DIEx nº 60-E5/CITEx, de 14 de janeiro de 2026, estudos e prospecções no sentido de verificar as ações necessárias para adequação da infraestrutura existente, apontando para a urgência de robustecer o ambiente de hospedagem visando processamento dedicado à IA a fim de garantir maior soberania digital no que se refere aos dados e sistemas utilizados no âmbito da Defesa Nacional. Nesse contexto, o CITEx informou ao Comitê de Governança Digital do Exército a necessidade de se realizar com celeridade contratações com intuito de:

3.3.1.1. **Adquirir Solução de Infraestrutura de IA (SIIA)**, compostos por servidores, *storages*, equipamentos de redes, licenças de *software* e demais componentes de TI; e

3.3.1.2. **Robustecer a infraestrutura do *Data Center* Corporativo localizado em Brasília**, de forma a permitir sua adequação em termos de espaço físico, climatização, estrutura elétrica, controle de acesso, capacidade de rede de dados e de armazenamento, visando ofertar capacidade de hospedagem de SIIA.

3.3.2. Após trabalho de prospecção tecnológica com os principais fabricantes de servidores com GPU, foram identificados cenários para atender as principais demandas de infraestrutura de processamento de cargas de trabalho de IA (item 3.2.6), sendo tratados pelo CITEx como Solução de Infraestrutura de IA (SIIA), com capacidade de até 48 GPU (NVIDIA modelo H200 ou B300) e alta demanda de consumo elétrico (da ordem de 65 kVA por rack).

3.3.3. Assim, considerando as demandas de curto prazo como a do CENSIPAM, a do EBOT e outras vindouras, é latente a necessidade de investimento tempestivo para o *retrofit* do *Data Center* Ricardo Franco e assim permitir manutenção da capacidade de hospedagem de novos sistemas corporativos do Exército Brasileiro, inclusive os suportados por IA ou que entregam capacidade de IA.

3.3.4. Diante desse cenário, complementando ao que foi apontado no item 2.1, a infraestrutura atual torna-se o principal gargalo para a hospedagem de novos equipamentos de voltados para IA, sendo imprescindível adaptação ou expansão estrutural da capacidade elétrica e refrigeração, adotando os pilares a seguir, a fim de permitir oferta de capacidade de hospedagem:

3.3.4.1. Densidade Elétrica Extrema: expandir a entrada de energia e atualizar a distribuição interna (PDUs de alta capacidade) é o único caminho para evitar quedas e sobrecargas (enquanto *racks*

tradicionais operam entre 5kW e 10kW, ambientes preparados para IA precisam suportar de 30kW a 100kW por *rack*).

3.3.4.2. Revolução na Refrigeração: adaptar o *data center* para tecnologias de ***Rear Door Heat Exchangers*** (RDHx) com possível evolução para ***Liquid Cooling*** (resfriamento líquido direto no processador) é essencial para manter a eficiência operacional e evitar redução de performance devido ao calor (o resfriamento a ar convencional já não é suficiente para dissipar o calor gerado por processamentos massivos).

3.3.4.3. Eficiência e Sustentabilidade (PUE): adaptar a infraestrutura permite adotar sistemas que reduzem o desperdício de energia, garantindo que o crescimento da capacidade de processamento não inviabilize financeiramente a operação devido à conta de luz.

3.4. Decisão do CGD do Exército Brasileiro sobre a contratação:

3.4.1. Diante do cenário apresentado pelo CITEx, o Comitê de Governança Digital (CGD) do Exército Brasileiro aprovou o prosseguimento do projeto e que o tema seja submetido ao Conselho Superior de Tecnologia da Informação (CONTIEx) e ao Alto Comando do Exército.

3.4.2. A aludida aprovação está registrada em Ata de Reunião do CGD, de 23 de fevereiro de 2026.

4. Área requisitante

Área Requisitante	Responsável
Divisão de Projetos e Inovação do CITEx	José Eduardo França
Divisão Técnica do 7° CTA	Matheus Mota Pires

5. Necessidades de Negócio

5.1. A presente contratação tem por finalidade viabilizar a melhoria e a ampliação da infraestrutura do *Data Center* Corporativo do Exército Brasileiro, em Brasília-DF, de forma a suportar processamento computacional especializado para Inteligência Artificial, com preservação dos atributos de disponibilidade, redundância, segurança física, continuidade operacional e conformidade com a certificação Tier III do *Uptime Institute*. Nesse contexto, os pilares de negócio da contratação compreendem: a expansão da capacidade de hospedagem por meio de nova sala segura; a ampliação da oferta energética e da capacidade de refrigeração; a manutenção e recertificação Tier III em *Design* e *Facilities*; e a garantia com suporte técnico por 12 meses.

5.2. A solução deverá adotar, como diretriz de negócio, um design híbrido adaptativo, apto a sustentar o ambiente definitivo de processamento de IA, com infraestrutura compatível com 12 *racks* de alta densidade, preservando a continuidade da operação do *data center* atual e permitindo evolução tecnológica da climatização, de *air cooling* para *liquid cooling*, quando necessário. A contratação também deverá contemplar, quando exigido pela condição atual do ambiente, a recuperação, reparação ou substituição de equipamentos e periféricos existentes, tendo em vista que o *Data Center* Ricardo Franco já possui quase 10 anos de operação.

5.3. Para fins de dimensionamento do ambiente final a ser suportado pela contratação, devem ser observados os seguintes parâmetros de referência:

Parâmetro	Referência
Quantidade total de racks de processamento de IA	12
Densidade elétrica por rack	65 kVA
Carga crítica total de TI	780 kVA
Carga de planejamento com margem de segurança	até 800 kVA
Altura do rack	44U
Profundidade do rack	1200 mm
Largura do rack	800 mm
Servidores de referência por rack	4 unidades
Altura ocupada pelos servidores por rack	40U
Peso total estimado por rack	800 a 1.500 kg
Carga concentrada para 12 racks	aprox. 10 a 12 ton
Recomendação de piso em áreas de alta densidade	superior a 1.200 kg/m^2
Capacidade de carga estrutural do rack, conforme tabela do documento	1.200 kg a 1.500 kg
Autonomia mínima da iluminação de emergência	5 horas
Quantidade mínima adicional de racks de Telecom	2

5.4. Os parâmetros acima fundamentam os requisitos de energia, climatização, piso, organização física, conectividade, monitoramento e segurança do ambiente de IA. Também será utilizado como referência um servidor de alta densidade, previsto para ser instalado, do tipo HPE *Cray Supercomputing* XD690, em configuração *air-cooled* de 10U, com até 12 fontes de 3.200 W, indicando que um *rack* com 4 equipamentos desse tipo, somados PDUs e *switches*, pode exceder 70 kW, razão pela qual o confinamento de corredor é tratado como requisito obrigatório. Abaixo estão listados os requisitos de negócio necessários para o planejamento da contratação.

5.4.1. Os requisitos de negócio da presente contratação deverão ser interpretados e desenvolvidos em consonância com a EAP do empreendimento, com os objetivos estratégicos da Força e da Defesa Nacional, bem como com as expectativas e determinações dos *stakeholders* institucionais envolvidos.

5.5. Capacidade de processamento computacional para Inteligência Artificial:

5.5.1. A infraestrutura a ser contratada deverá prover ambiente de hospedagem de ativos de TI com capacidade de processamento computacional especializado para aplicações de Inteligência Artificial, aprendizado de máquina, análise avançada de dados, visão computacional, automação, inferência e treinamento de modelos, em ambiente próprio e controlado pela Administração.

5.5.2. A solução deverá ser apta a suportar 12 *racks* de alta densidade, com capacidade individual de até 65 kVA, totalizando carga crítica de TI de 780 kVA, considerada capacidade de planejamento de até 800 kVA, de forma compatível com a operação de servidores de última geração voltados ao processamento intensivo por GPU. O ambiente deverá viabilizar a implantação, execução, treinamento, ajuste e operação de modelos de IA com desempenho compatível com as necessidades institucionais atuais, com redução do tempo de processamento, aumento da eficiência dos serviços digitais e maior autonomia tecnológica da Força.

5.5.3. Deverá, ainda, assegurar maior controle sobre dados, modelos, fluxos de processamento e ambientes de execução, em observância aos requisitos institucionais de segurança da informação, disponibilidade, proteção de ativos estratégicos e soberania tecnológica.

5.6. Elaboração de Projeto Executivo:

5.6.1. A contratação deverá contemplar a elaboração de Projeto Executivo, com nível de detalhamento suficiente para evitar inadequações estruturais, garantir a integridade da nova sala segura e assegurar a compatibilidade entre os diversos subsistemas da expansão do *Data Center*.

5.6.2. O projeto deverá abranger, no mínimo, os seguintes projetos setoriais: civil, elétrico, sala segura, climatização, sistema de proteção e combate a incêndio, rede passiva, monitoramento, moving, recuperação das adaptações civis, limpeza e paisagismo. Deverão também apresentar a capacidade máxima de instalação de PODs de processamento de IA, de modo a subsidiar estudos futuros de ampliação da infraestrutura.

5.6.3. Antes da elaboração do Projeto Executivo deverá ser estruturado o modelo de solução para permitir transição entre tecnologias de resfriamento, prevendo desde já as condições de base para eventual evolução de *air cooling* para *liquid cooling*, sem exigir, nesta fase, a implantação imediata de toda a infraestrutura de resfriamento líquido.

5.6.4. O Projeto executivo deve ser detalhadamente apresentado para a Equipe técnica responsável do 7° CTA e CITEx e sua execução ficará condicionada à aprovação do Projeto.

5.7. Requisitos de Energia elétrica, potência e continuidade operacional:

5.7.1. A solução deverá assegurar fornecimento contínuo, estável e seguro de energia elétrica para suportar a carga crítica do ambiente de IA, dimensionado para 12 *racks* de alta densidade, com carga crítica total de TI de 780 kVA e planejamento de até 800 kVA. Para isso, deverá contemplar infraestrutura elétrica compatível com ambiente de missão crítica, incluindo subestação interna, *radiers*, grupos moto geradores, tanques de combustível, UPS, quadros elétricos, PDUs e cabeamento elétrico necessário ao sistema.

5.7.2. A entrada de energia existente encontra-se dimensionada em potência instalada de 6.178,84 kW e potência demandada de 2.273,55 kVA. Assim, havendo necessidade de ajuste para suportar adequadamente a expansão, caberá à contratada, com apoio do contratante, promover as tratativas e aprovações necessárias junto à concessionária de energia.

5.7.3. Os sistemas de alimentação ininterrupta deverão ser modulares, redundantes e do tipo *True On-Line*, com baterias para proteção de cargas sensíveis, devendo o chassi principal ser dimensionado para a carga final do ambiente. A solução de geração deverá prever redundância e autonomia compatíveis com a criticidade do processamento de IA, podendo inclusive considerar a integração da capacidade dos dois geradores atualmente existentes de 1000 kVA, cuja referência é de 200 kVA, desde que isso se mostre técnica e economicamente adequado. Inclui-se, ainda, a verificação da necessidade de substituição de estabilizadores, baterias e demais componentes associados, bem como o melhor aproveitamento do espaço técnico já reservado para os sistemas UPS, de modo a reduzir, sempre que tecnicamente viável, a necessidade de implantação de soluções adicionais em área externa.

5.7.4. Deve ser analisada a capacidade e necessidade de expansão dos atuais tanques de combustível para que após a instalação dos novos geradores ainda seja possível ter uma autonomia mínima de 12 (doze) horas, conforme previsto para a certificação Tier III.

5.7.5. A solução deverá também prover Sistema de Proteção contra Descargas Atmosféricas (SPDA), quadros elétricos e distribuição interna por PDUs de alta capacidade, de forma a evitar sobrecargas, preservar a qualidade de energia e viabilizar a operação segura de cargas de alta densidade computacional.

5.7.6. A contratação deverá contemplar a melhoria da infraestrutura elétrica da Sala TCOM, com adequações necessárias à segurança, continuidade operacional, organização e compatibilização com a expansão do ambiente crítico do *Data Center*.

5.8. Requisito de resfriamento e climatização de alta capacidade:

5.8.1. A contratação deverá garantir condições térmicas adequadas ao funcionamento contínuo e seguro dos equipamentos do ambiente de IA, com capacidade de dissipação compatível com *racks* de até 65 kVA, em arquitetura final de 12 racks. A solução deverá operar com *air cooling* de precisão assistido por *chillers*, em ambiente confinado, com redundância N+1 e foco na obtenção do melhor indicador possível de eficiência energética do *Data Center*.

5.8.2. Considerando a elevada densidade térmica do ambiente, deverá prever o confinamento da climatização, em *layout* físico que favoreça a separação de fluxos térmicos, bem como a adoção de tecnologias de resfriamento de alta capacidade. Pelas prospecções realizadas verificou-se que a melhor tecnologia para operar em conjunto com as máquinas *In-Row* seria o trocador de calor tipo *Rear Door*.

5.8.3. A solução deverá, ainda, preservar a coexistência tecnológica entre *air cooling* e futura adoção de *liquid cooling*, mediante previsão, nos projetos conceitual e executivo, de espaço para coletores de distribuição de

água, tubulações em aço inoxidável para o sistema de resfriamento técnico, válvulas de bloqueio e engates rápidos em cada posição de *rack*, possibilitando futura instalação de CDUs específicos, sem obrigatoriedade de implantação imediata desses componentes nesta etapa. Destaca-se, inclusive, a possibilidade futura de suportar GPUs de alta demanda energética, como arquiteturas equivalentes à NVIDIA *Blackwell* superiores a 1000 W por componente.

5.8.3.1. A arquitetura de climatização deverá considerar, preferencialmente, chillers indoor instalados em área técnica protegida, com condensadoras externas/remotas, de modo a reduzir a exposição dos principais componentes elétricos, mecânicos e de controle às condições climáticas externas, melhorar a manutenibilidade, favorecer circuitos hidráulicos mais curtos e permitir controle mais preciso da temperatura do fluido de resfriamento próximo às cargas críticas de TI.

5.8.4. O sistema de climatização deverá, sempre que tecnicamente aplicável, prever estratégias de *free-cooling* de aproveitamento de condições externas favoráveis, com vistas à redução do consumo energético e ao aumento da eficiência operacional do *Data Center*.

5.8.5. O sistema de resfriamento técnico deverá prever, quando aplicável, solução de tratamento do fluido térmico, com recursos de filtragem, controle de qualidade e dosagem química automática, destinada à prevenção de corrosão, incrustações e contaminação biológica nas tubulações e equipamentos.

5.8.6. A contratação deverá contemplar a melhoria da climatização da Sala TCOM, assegurando condições ambientais compatíveis com os ativos ali instalados, com foco em confiabilidade, organização do ambiente e integração à infraestrutura crítica do *Data Center*.

5.9. Sala segura para núcleo de IA:

5.9.1. A contratação deverá prover sala modular segura para o núcleo de processamento de IA, com proteção compatível com a criticidade dos ativos hospedados, observando requisitos de estabilidade, estanqueidade, proteção contra água, pó e fogo, além de compatibilidade com as exigências gerais da certificação Tier III.

5.9.2. Toda a estrutura da sala segura, incluindo paredes, teto, piso e porta, deverá garantir resistência ao fogo por no mínimo **120 (cento e vinte) minutos**, bem como estanqueidade suficiente para que o agente extintor permaneça no ambiente pelo tempo necessário à extinção do incêndio. A solução deverá observar as normas **NFPA 2001** e **NFPA 75**, ou normas ABNT correspondentes, e incluir acabamento com pintura antichama também nas salas técnicas adjacentes, especialmente UPS e Telecom, com o objetivo de ampliar a resistência a sinistros externos.

5.10. Organização física, *racks* e infraestrutura de piso:

5.10.1. O ambiente deverá ser organizado para acomodar os 12 (doze) *racks* de processamento em 2 (duas) fileiras, de modo a permitir o confinamento da climatização e o ganho de eficiência térmica. Os *racks* de referência do sistema deverão possuir 44U de altura, 1200 mm de profundidade e 800 mm de largura, permitindo acomodação adequada dos equipamentos, da curvatura dos cabos de alta performance e da instalação lateral de PDUs de 60A/80A.

5.10.1.1. Os *racks* e sua infraestrutura associada deverão possuir caráter agnóstico quanto ao fabricante dos equipamentos de TI, observando padrões técnicos de mercado e normas aplicáveis de fixação, acomodação e interoperabilidade física.

5.10.1.2. Serão também inclusos *racks* para composição de até 2 (dois) POD Padrão (sem ser de IA).

5.10.1.3. A disposição física e a montagem dos *racks* deverão observar solução de *layout* que maximize o aproveitamento das áreas de expansão previstas, sem prejuízo dos requisitos de confinamento térmico, manutenção, circulação segura e expansão futura.

5.10.2. Considera-se, como referência técnica, a ocupação de cada *rack* com 4 (quatro) servidores, equivalentes a 40U, além de *switches*, PDUs e *patch panels*. Considera também, para fins de carga mecânica, peso aproximado de 200 kg por servidor, resultando em no mínimo 800 kg apenas em servidores por *rack*, com peso total estimado entre 800 e 1500 kg por *rack*, e carga total concentrada de aproximadamente 10 a 12

toneladas para o conjunto de 12 *racks*. Em razão disso, o piso das áreas de alta densidade deverá ser compatível com cargas superiores a 1.200 kg/m², e os *racks* deverão possuir capacidade estrutural compatível com o suporte do peso estático da infraestrutura interna, estimada na ordem de **1.200 kg a 1.500 kg** por *rack*.

5.10.3. O ambiente também deverá contar com iluminação adequada, por meio de luminárias tipo painel LED embutidas no forro modular, complementadas por blocos autônomos de iluminação de emergência com baterias de lítio e autonomia mínima de **5 horas**.

5.11. Requisitos de conectividade e rede passiva:

5.11.1. A solução deverá garantir conectividade resiliente, de alta capacidade e preparada para o tráfego intensivo de dados exigido pelo processamento de IA, contemplando a interligação entre servidores, ativos de rede, sistemas de armazenamento, sistemas de monitoramento e demais componentes da infraestrutura crítica, bem como a conectividade resiliente com órgãos e ambientes externos que demandem integração operacional segura, a exemplo do CENSIPAM, quando aplicável.

5.11.2. Deverão ser previstos, no mínimo, **2 *racks* adicionais de telecomunicações**, específicos para interligação dos servidores e ativos de rede do *cluster*, admitindo configuração como EDA (Equipment Distribution Area), em complemento ao *rack* de Core/MDA já existente no ambiente. A solução de rede passiva deverá prever DIOs modulares, capacidade óptica compatível com a necessidade dos sistemas de IA e uso obrigatório de soluções pré-conectorizadas, eliminando a necessidade de fusões em campo e favorecendo desempenho, padronização e menor tempo de implantação.

5.12. Requisito de monitoramento integrado do *Data Center*:

5.12.1. A contratação deverá contemplar nova solução de monitoramento integrada, abrangendo o ambiente atual do *Data Center* Ricardo Franco e a expansão destinada ao núcleo de IA. Todos os *softwares* envolvidos deverão ser novos, entregues configurados para operação e integrados aos subsistemas de ar-condicionado, UPS, GMG, incêndio e demais elementos de infraestrutura, por meio de dispositivo concentrador de alarmes com servidor *web* integrado e acesso via navegador. A visualização da solução deverá ser realizada em *videwall* instalado na sala de monitoramento do 7° CTA.

5.12.2. A plataforma de DCIM deverá permitir visualização 3D navegável, gestão completa do inventário de ativos, representação de elevação dos *racks*, mapas termográficos em tempo real, acompanhamento de temperatura, umidade, *status* de portas, presença de líquidos, consumo elétrico, tensão, corrente e balanceamento de fases, bem como geração de alarmes visuais e sonoros e envio de notificações por *e-mail* e *traps* SNMP. O painel central de incêndio deverá permanecer integrado ao sistema de monitoramento ambiental, fornecendo alertas e diagramas em tempo real.

5.12.3. A solução deverá contar com sensores individuais em todos os *racks* e áreas técnicas, incluindo, no mínimo, **2 (dois) sensores de temperatura e umidade por *rack*** em todo o *Data Center*, além de sensores adicionais para a sala elétrica e a sala de telecomunicações. Também deverão ser instalados sensores de detecção de líquidos sob o piso elevado, em pontos estratégicos, para identificação imediata de vazamentos e infiltrações.

5.12.4. A solução de monitoramento poderá considerar, quando tecnicamente adequado, o aproveitamento de dispositivos e sensores já existentes no ambiente, mediante calibração, integração, adequação ou substituição, de forma a preservar a confiabilidade operacional e a economicidade da contratação.

5.13. Requisito de proteção e combate a incêndio:

5.13.1. A contratação deverá prover sistema de detecção e combate a incêndio adequado a ambiente de missão crítica, com capacidade de identificação precoce de eventos, mínima interferência sobre os ativos de TIC e integração plena com a solução de monitoramento e segurança do ambiente.

5.13.2. O sistema deverá contemplar detecção refinada do tipo *High Sensitivity Smoke Detection* (HSSD), apta a identificar partículas de fumaça em níveis muito baixos de obscuridade, inclusive em ambientes com alta

renovação de ar. Também deverá prever detecção em ambiente principal, entrepiso, entreforro e, obrigatoriamente, na área de confinamento do corredor frio dos *racks*. O sistema deverá dispor de acionamento manual direto, preferencialmente com atuação independente de falhas elétricas ou eletrônicas do sistema.

5.13.3. O combate deverá utilizar agente extintor limpo, sem resíduos, de alta resistência dielétrica e compatível com equipamentos de TI, observadas as normas correspondentes. O sistema deverá dispor de acionamento manual direto, estações manuais de ***ABORT***, lógica cruzada para descarga apenas após atuação de dois ou mais detectores e comando automático de liberação das travas magnéticas das portas em situação de incêndio, de modo a garantir segurança e evacuação.

5.13.4. O requisito de proteção, detecção e combate a incêndio encontra-se contemplado no item 1 da contratação, referente à expansão da capacidade do Data Center com implantação da nova Sala Segura, constituindo subsistema integrante desse ambiente. Seu detalhamento técnico encontra-se estabelecido no Apêndice I do Termo de Referência, não se tratando, portanto, de item autônomo da contratação.

5.13.5. A inclusão do referido subsistema decorre das características próprias da Sala Segura e da necessidade de proteção dos ativos de TIC nela hospedados. O item 4.3.1 do Anexo I da IN SGD/ME nº 94 /2022 inclui, na própria concepção de Sala Segura, sistemas de monitoramento ambiental, detecção e alarme de incêndio e demais subsistemas relacionados à proteção contra ameaças físicas. Dessa forma, sua previsão guarda relação direta e necessária com a implantação e o funcionamento seguro da Sala Segura e com a proteção dos equipamentos de TIC nela instalados.

5.14. Previsão hidráulica:

5.14.1. Prever no projeto executivo (o que não implica aquisição de material correspondente, muito menos sua implantação) espaço para instalação de coletores de distribuição de água e tubulações de aço inoxidável para o Sistema de Resfriamento Técnico (TCS), com pontos de conexão com válvulas de bloqueio e engates rápidos em cada posição de *rack*, permitindo a instalação futura de Unidades de Distribuição de Líquidos de Refrigeração (CDU) específicos.

5.15. Segurança física, controle de acesso e CFTV:

5.15.1. A solução final deverá contemplar mecanismos integrados de segurança orgânica do Data Center, incluindo controle de acesso restrito e monitoramento visual contínuo, abrangendo o ambiente interno e a área externa. O controle de acesso deverá utilizar leitores biométricos faciais e fechaduras eletromagnéticas, com integração aos demais sistemas e mecanismos de segurança, monitoramento e resposta a incidentes. Esses componentes deverão operar de forma integrada aos demais elementos da solução, constituindo parte indissociável da solução final do Data Center, necessária à sua segurança, disponibilidade e operação adequada.

5.15.2. O sistema de CFTV deverá integrar a solução final de segurança e monitoramento do Data Center, operando em regime 24x7, com capacidade de decodificação compatível com o Centro de Operações e integração aos demais mecanismos de segurança, controle de acesso e resposta a incidentes. Deverá incorporar recursos analíticos apoiados por IA, tais como reconhecimento facial, biometria comportamental, rastreamento de objetos, termografia integrada, detecção precoce de fumaça e chama por análise de pixels, alerta de porta de rack aberta por tempo excessivo e mapa de calor de movimentação, de forma a elevar a capacidade integrada de prevenção, monitoramento, auditoria e resposta a eventos físicos no ambiente.

5.15.3. Os componentes de segurança física, controle de acesso e CFTV, quando considerados isoladamente, enquadram-se nas exclusões previstas no item 1.5, alínea “b”, do Anexo II da IN SGD/ME nº 94/2022. Na presente contratação, contudo, tais componentes não constituem solução autônoma ou finalidade independente, mas subsistemas acessórios de proteção física indispensáveis à operação segura da Sala Segura e do Data Center de missão crítica.

5.15.4. Sua contratação conjunta justifica-se pela necessidade de integração com os sistemas de monitoramento ambiental, detecção e alarme de incêndio, controle de eventos e demais mecanismos de

proteção do ambiente, permitindo tratamento coordenado de incidentes, rastreabilidade, controle de acesso às áreas críticas e proteção dos ativos de TIC.

5.15.5. A segregação desses componentes da solução principal aumentaria os riscos de incompatibilidade entre plataformas, interfaces e dispositivos de segurança, bem como poderia fragmentar a responsabilidade pela integração, configuração, testes e funcionamento conjunto do ambiente. Por essa razão, embora reconhecida sua classificação específica à luz do item 1.5, “b”, do Anexo II, mantém-se demonstrada sua pertinência técnica e necessária integração à solução contratada.

5.16. Certificação Tier III do *Uptime Institute*:

5.16.1. A expansão da capacidade do *data center* deverá preservar a classificação Tier III já existente no ambiente atual, mantendo a aderência aos critérios do *Uptime Institute Tier Standard: Topology*, de modo que a infraestrutura expandida permaneça *concurrently maintainable*, sem interrupção da operação de TI durante intervenções planejadas de manutenção em quaisquer componentes ou caminhos de distribuição críticos.

5.16.2. O projeto de expansão deverá ser concebido, implantado e comissionado de forma a não descaracterizar a topologia certificada do ambiente atual, devendo eventuais alterações em arquitetura elétrica, mecânica, de resfriamento, distribuição ou suporte à carga crítica ser compatíveis com a manutenção da certificação Tier III.

5.16.3. Sempre que a expansão impactar elementos associados à topologia certificada, deverá ser prevista a submissão da documentação de projeto e da implantação às etapas de avaliação cabíveis do *Uptime Institute*, especialmente quanto à conformidade entre o desenho da expansão e a infraestrutura efetivamente construída, em linha com os processos de *Tier Certification of Design Documents* e *Tier Certification of Constructed Facility*.

5.16.4. A solução adotada deverá assegurar que a ampliação da capacidade elétrica, térmica, física e lógica do ambiente, inclusive para suportar cargas de processamento de IA, ocorra sem perda dos atributos de disponibilidade, redundância e manutenibilidade concorrente exigidos para instalações Tier III.

5.17. Recomposição das áreas externas e paisagísticas:

5.17.1. A contratação deverá contemplar a recomposição das áreas externas eventualmente afetadas pelas intervenções necessárias à implantação da expansão do *data center*, incluindo, quando aplicável, a recuperação de gramados, jardins, cobertura vegetal, arborização, calçadas, meios-fios, pisos externos e demais elementos urbanísticos impactados pela execução das obras e instalações.

5.17.2. A solução deverá assegurar que, após a conclusão dos serviços, as áreas atingidas sejam restabelecidas em condições iguais ou superiores às originais, observando-se padrões adequados de acabamento, segurança, drenagem, estabilidade do solo, acessibilidade e harmonização com a infraestrutura existente.

5.17.3. Quando houver supressão, remanejamento ou dano a elementos vegetais, a contratação deverá prever sua devida recomposição, replantio, substituição ou recuperação, conforme as condições do local e as exigências técnicas e normativas aplicáveis, de modo a mitigar impactos físicos, ambientais e paisagísticos decorrentes da implantação da solução.

5.17.4. A recomposição externa deverá também contribuir para a segurança orgânica do *data center*, restringindo a visibilidade direta de ativos críticos a partir do perímetro externo, mitigando o impacto visual das estruturas industriais implantadas e promovendo adequada harmonização urbanística, paisagística e ambiental do conjunto.

5.18. Requisito de implantação, *mooving* e documentação:

5.18.1. A contratação deverá prever as condições necessárias à movimentação de ativos e à migração dos sistemas críticos para o novo ambiente, incluindo servidores, *switches*, *storages* e, quando aplicável, máquinas virtuais, com planejamento orientado à minimização de *downtime* e à preservação da continuidade do negócio.

5.18.2. Deverá ser incluído seguro de transporte que assegure a reposição de equipamentos idênticos em caso de dano durante a movimentação. Ao término da implantação, deverá ser produzida documentação ***as built*** detalhada e identificações de toda a engenharia executada, apta a subsidiar operação, manutenção, auditoria e futuras intervenções no ambiente.

5.19. Requisito para expansão de novos POD Padrão:

5.19.1. Além da instalação do POD de IA na sala segura a ser construída, está sendo prevista a possibilidade de instalação de 2 (dois) novos POD de *Rack* Padrão, para absorver demandas operacionais futuras cujos equipamentos/servidores necessitem de carga de TI menor.

5.19.1. Desta forma a contratação permitirá ocupar as áreas disponíveis do *data center*, otimizando a infraestrutura instalada.

5.19.2. A instalação de novos POD pode ocorrer tanto na área da nova sala segura, quanto no espaço do *Data Hall*, totalizando 2 (dois) POD padrão com até 12 *racks* (11 *racks* TI + 1 Telecom).

5.20. Condições de execução e pagamento:

5.20.1. Como regra de execução orientada a resultado, os pagamentos relativos às entregas e serviços da contratação, excetuados os projetos a serem entregues, deverão observar a condição de recertificação **Tier III *Design*** junto ao *Uptime Institute*.

5.20.2. Além disso, eventuais ajustes de contrato voltados à melhor execução do projeto poderão ser propostos, desde que respeitados o edital e seus anexos e desde que haja concordância do contratante, especialmente no que se refere à granulação de atividades executivas e ao desembolso financeiro.

5.21. Longevidade e Manutenção dos equipamentos:

5.21.1. As soluções tecnológicas para o ecossistema do DC RF deve priorizar, de forma **mandatória**, sistemas e equipamentos que exijam menor intensidade de manutenção preventiva e corretiva ao longo de seu ciclo de vida, visando a longevidade dos bens, a necessidade de mitigar os riscos decorrentes da persistente dificuldade de retenção e contratação de pessoal técnico qualificado para operação de ambientes de missão crítica, desde que o seu Custo Total de Propriedade (TCO) decenal seja inferior ou igual.

6. Necessidades Tecnológicas

6.1. Caracterização da demanda tecnológica:

6.1.1. A presente contratação tem como necessidade tecnológica central a expansão da infraestrutura do *Data Center* Coronel Ricardo Franco (DC RF), de forma a permitir a sustentação de cargas computacionais intensivas voltadas ao processamento de Inteligência Artificial (IA), incluindo treinamento, ajuste fino, inferência, processamento massivo de dados, modelos de linguagem de grande porte, bases vetoriais, aplicações generativas e demais *workloads* associados a ambientes de IA de uso estratégico.

6.1.2. A demanda não se limita à ampliação convencional de capacidade de hospedagem de sistemas corporativos. Trata-se de preparar o DC RF para receber infraestrutura computacional de alta densidade, composta por servidores acelerados por GPU, redes de interconexão de alta velocidade, armazenamento de elevado desempenho, sistemas de energia crítica, climatização de precisão e mecanismos de continuidade operacional compatíveis com a criticidade das cargas de trabalho pretendidas.

6.1.3. Diferentemente de ambientes tradicionais de TIC, nos quais a densidade média por *rack* tende a ser menor e distribuída, os ambientes voltados à Inteligência Artificial concentram elevada carga elétrica e térmica em poucos *racks*. Essa característica exige uma infraestrutura específica, capaz de suportar alta potência por *rack*, alto volume de calor dissipado, resfriamento contínuo, baixa tolerância a falhas, alta disponibilidade e escalabilidade tecnológica.

6.1.4. Dessa forma, a solução tecnológica pretendida deverá viabilizar a instalação de um POD de IA em Sala Segura com aproximadamente 130 m², composta por 12 *racks* de TI de alta densidade, com capacidade térmica estimada de até 65 kW por *rack*, além de 2 *racks* de Telecom, de modo a permitir a acomodação segura, estável e evolutiva de equipamentos destinados ao processamento massivo de IA.

6.2. Prospecção tecnológica dos AI PODs:

6.2.1. Para subsidiar a definição da necessidade tecnológica e identificar a alternativa com melhor relação entre desempenho, custo e aderência à demanda institucional, foi realizada prospecção com fabricantes e fornecedores especializados em infraestrutura de IA, considerando diferentes configurações de AI PODs, aqui compreendidos como conjuntos convergentes de servidores, GPUs, interconexão, armazenamento e demais componentes voltados ao processamento de IA.

6.2.2. A prospecção considerou, como referência, quatro classes de AI PODs, tipificadas em tamanhos **P, M, G e GG**, cada uma associada a diferentes níveis de maturidade, desempenho e tipos de *workload* de IA.

Tipo Server	Qtd GPU	Modelo GPU	Custo médio por GPU (R$)	Btoken	EPM	custo EPM (R$)/Btoken	Processamento Massivo	Custo-Benefício
P	4	NVIDIA L40S	2.209.975,00	13	1,2	1.841.645,83	Baixa (Foco: Inferência/RAG)	Caro para Processamento Massivo
M	4	NVIDIA H100 NVL	2.498.450,00	70	3,5	713.842,86	Média (Foco: LLMs Médios)	Equilibrado para modelos médios
G	8	NVIDIA L40S	2.142.737,50	70	2,4	892.807,29	Média-Alta (Foco: Densidade)	Baixo Custo-Benefício para Processamento Massivo
GG	8	NVIDIA H200	2.464.148,13	175	5,4	456.323,73	Alta (Foco: Treinamento)	MELHOR CUSTO-BENEFÍCIO
ULTRA	8	NVIDIA B300	não foi cotado	500	10,0		Ultra (Foco em aprendizado e treinamentos)	Obs: equipamento apenas para Rfr técnica

6.2.3. A tipificação adotada permitiu comparar configurações destinadas a diferentes finalidades:

6.2.3.1. **Tipo P**: voltado a cargas de menor intensidade, com foco predominante em inferência e aplicações com RAG;

6.2.3.2. **Tipo M**: voltado a modelos médios e aplicações de IA com demanda intermediária;

6.2.3.3. **Tipo G**: voltado a cargas médias-altas, com foco em maior densidade computacional; e

6.2.3.4. **Tipo GG**: voltado a processamento massivo, com foco em treinamento, ajuste de modelos e cargas de IA de maior complexidade.

6.2.4. A análise demonstrou que, para a necessidade tecnológica do Exército Brasileiro, o foco não deve ser apenas a disponibilização de capacidade pontual de inferência, mas sim a criação de infraestrutura com capacidade de processamento massivo, preparada para treinamento, ajuste fino, processamento de grandes volumes de dados e sustentação de modelos de maior porte.

6.3. Métricas utilizadas para avaliação tecnológica:

6.3.1. Para comparar as configurações prospectadas, foram utilizadas métricas de custo e desempenho, especialmente o **custo médio por GPU**, a quantidade de parâmetros processáveis em bilhões de *tokens* ou parâmetros de referência, denominada na análise como ***Btoken***, e a métrica de **Eficiência de Processamento Massivo (EPM)**.

6.3.2. A métrica EPM foi adotada por refletir não apenas a quantidade bruta de GPUs, mas também a qualidade da arquitetura computacional, a geração do *chip*, a capacidade de interconexão, o desempenho de memória e a aptidão da solução para cargas de processamento massivo.

6.3.3. No contexto de IA, a simples contagem de GPUs não é suficiente para caracterizar a capacidade real da solução. Aspectos como geração tecnológica do acelerador, largura de banda de memória, capacidade de

comunicação entre GPUs, suporte a treinamento distribuído, desempenho em precisão reduzida, eficiência energética e maturidade da arquitetura tem impacto direto na capacidade efetiva de processamento.

6.3.4. Nesse sentido, a análise considerou que arquiteturas de geração mais recente, como aquelas baseadas em GPUs da classe H200, apresentam vantagem tecnológica em relação a gerações anteriores, em razão de maior capacidade de memória, maior largura de banda e melhor adequação a modelos de IA de grande porte.

6.3.5. Para fins de comparação, observou-se que a solução do tipo **GG**, referenciada com 8 GPUs da classe H200, apresentou o melhor indicador de custo-benefício para processamento massivo, com menor custo por unidade de eficiência de processamento em relação às demais alternativas avaliadas.

6.4. Justificativa da necessidade de processamento massivo de IA:

6.4.1. A necessidade tecnológica identificada demanda capacidade de processamento massivo porque as futuras aplicações de IA do Exército Brasileiro poderão envolver grandes bases de dados, modelos de linguagem, análise de documentos, apoio à decisão, sistemas de busca semântica, geração de respostas assistidas, processamento de imagens, análise de séries temporais, correlação de eventos, automação de processos, apoio logístico, aplicações de comando e controle e outras soluções que exigem elevado desempenho computacional.

6.4.2. Em ambientes dessa natureza, a infraestrutura computacional precisa ser capaz de processar grande volume de dados de forma simultânea, reduzir tempos de treinamento e inferência, permitir testes interativos de modelos, executar *pipelines* de dados e manter capacidade disponível para múltiplos projetos institucionais.

6.4.3. A escolha de uma infraestrutura subdimensionada poderia limitar o desenvolvimento de soluções de IA, restringir a execução de modelos mais complexos, aumentar o tempo de processamento, elevar custos operacionais por retrabalho, gerar necessidade prematura de nova expansão e comprometer a efetividade da estratégia institucional de IA.

6.4.4. Dessa forma, a necessidade tecnológica não se restringe à instalação física de *racks*, mas envolve a criação de uma infraestrutura de alta densidade capaz de sustentar, com segurança e continuidade, equipamentos compatíveis com AI PODs de maior desempenho, especialmente aqueles classificados como tipo **GG**, voltados ao processamento massivo e ao treinamento de modelos.

6.4.5. A contratação possui caráter estratégico, na medida em que busca ampliar a capacidade, a disponibilidade e a resiliência da infraestrutura tecnológica que suporta sistemas e serviços essenciais à organização. A evolução das aplicações institucionais, associada ao crescimento da demanda por processamento, armazenamento e análise de dados, impõe a necessidade de preparação da infraestrutura para novos cenários tecnológicos.

6.4.6. A **Portaria GM-MD nº 4.360/2026**, ao instituir a Política de Inteligência Artificial de Defesa, estabelece como princípios, entre outros, a busca pela autonomia tecnológica, a segurança operacional, a resiliência em ambientes contestados, a inovação, a interoperabilidade e a padronização. Esses princípios reforçam a necessidade de que infraestruturas destinadas a hospedar sistemas críticos da Defesa sejam concebidas com elevados níveis de disponibilidade, redundância, segurança e capacidade de evolução tecnológica.

6.4.7. Assim, a presente contratação não se limita ao atendimento de uma necessidade imediata de expansão de capacidade, mas busca estabelecer infraestrutura apta a suportar a evolução tecnológica e operacional da Força, reduzindo riscos de indisponibilidade, obsolescência e insuficiência de capacidade

6.5. Justificativa técnica pela referência ao AI POD tipo GG:

6.5.1. A prospecção realizada indicou que o AI POD tipo **GG** apresenta a melhor relação de custo-benefício para a demanda pretendida, pois combina maior capacidade de processamento, arquitetura de GPU mais moderna, maior EPM e menor custo relativo por unidade de processamento massivo.

6.5.2. Embora o custo médio por GPU do tipo **GG** seja superior ao de algumas configurações de menor porte, a análise de eficiência demonstra que o custo por EPM/ *Btoken* é inferior, o que indica melhor aproveitamento do investimento quando a finalidade é processamento massivo de IA.

6.5.3. Em outras palavras, soluções de menor porte podem apresentar menor custo unitário inicial, mas tendem a oferecer menor eficiência para cargas intensivas, tornando-se menos vantajosas quando avaliadas sob a ótica de desempenho agregado, escalabilidade, tempo de processamento e capacidade de atendimento a modelos mais complexos.

6.5.4. A solução do tipo **P**, por exemplo, apresenta foco em inferência e RAG, sendo considerada cara para processamento massivo. A solução do tipo **M** mostra-se equilibrada para modelos médios, mas não representa a melhor opção para treinamento e processamento de maior escala. A solução do tipo **G** apresenta foco em densidade, mas com custo-benefício inferior para processamento massivo quando comparada à solução do tipo **GG**. Já a solução **Ultra**, embora possua potencial tecnológico superior, foi considerada apenas como referência técnica, por não ter sido cotada e por estar associada a cenário de ultra processamento e aprendizado de maior complexidade.

6.5.5. Assim, considerando a demanda institucional de processamento de IA, a necessidade de preparar o DC RF para cargas futuras e a análise de custo-benefício por eficiência de processamento, a referência tecnológica do AI POD tipo **GG** mostra-se a mais aderente à necessidade tecnológica mapeada.

6.5.6. Ressalta-se que essa referência não implica, por si só, restrição indevida a marca ou modelo específico no instrumento convocatório. No âmbito do ETP, a referência ao tipo GG serve para dimensionar a infraestrutura necessária de energia, climatização, espaço físico, cabeamento, *racks*, telecomunicações e continuidade operacional, devendo o Termo de Referência adotar especificações técnicas funcionais, desempenho mínimo e critérios de equivalência, quando aplicável.

6.6. Necessidade de infraestrutura física de alta densidade:

6.6.1. Considerando a referência tecnológica adotada, a infraestrutura a ser implantada deverá suportar um ambiente de alta densidade, com previsão de POD de IA composto por 12 *racks* de TI, com capacidade estimada de até 65 kW por *rack*, além de 2 *racks* de Telecom.

6.6.2. Essa necessidade decorre da concentração de servidores acelerados por GPU em poucos *racks*, o que gera elevada demanda elétrica e térmica. Em um ambiente convencional, cargas dessa magnitude não poderiam ser absorvidas apenas por infraestrutura tradicional de climatização e distribuição elétrica.

6.6.3. A nova Sala Segura deverá, portanto, ser concebida com capacidade física, elétrica, térmica e lógica compatível com esse padrão de densidade, incluindo piso, rotas de cabeamento, barramentos, quadros elétricos, sistemas de climatização de precisão, monitoramento ambiental, controle de acesso, combate a incêndio e integração com a infraestrutura existente do DC RF.

6.6.4. A necessidade de utilização de área já prevista para expansão do DC RF também se justifica por permitir a implantação do novo ambiente dentro de perímetro controlado, aproveitando a governança, segurança, conectividade e operação já existentes, além de preservar o caráter estratégico e próprio da infraestrutura.

6.7. Necessidade de energia crítica e geração redundante:

6.7.1. A demanda tecnológica de IA implica aumento expressivo da carga elétrica do *data center*, especialmente em razão dos servidores acelerados por GPU, dos sistemas de armazenamento, das redes de alta velocidade, dos equipamentos de Telecom e dos sistemas de climatização associados.

6.7.2. Para atender a essa demanda, a infraestrutura elétrica deverá ser ampliada de forma compatível com ambiente de missão crítica, contemplando alimentação, transformação, distribuição, UPS, barramentos, proteção, chaveamento, paralelismo de geradores e redundância.

6.7.3. Considerando a infraestrutura existente, composta por 2 (dois) grupos geradores de 1 MVA, e a disponibilidade de *slots* de expansão compatíveis com o mesmo padrão, a solução tecnológica adotará a ampliação para quatro grupos geradores de 1 MVA, operando em paralelismo na configuração 3 + 1, totalizando 3 MVA de capacidade ativa e uma unidade redundante.

6.7.4. Essa configuração N+1 mostra-se adequada à necessidade tecnológica e à busca de certificação Tier III, pois permite maior disponibilidade, manutenção planejada e resiliência da infraestrutura, ao mesmo tempo em que evita os riscos estruturais associados à instalação de geradores de maior porte, como unidades de 1,5 MVA, cujo peso poderia impor esforços adicionais sobre a laje técnica existente.

6.7.5. A escolha por geradores de 1 MVA também é mais compatível com o padrão construtivo já existente, reduz riscos de implantação, tende a apresentar melhor economicidade e permite evolução da geração de energia sem descaracterizar a infraestrutura prevista para o sítio.

6.8. Necessidade de climatização de alta densidade e arquitetura híbrida:

6.8.1. A carga térmica estimada para o POD de IA exige solução de climatização específica para alta densidade, não sendo adequada a utilização exclusiva de sistemas tradicionais de ar-condicionado de precisão concebidos para cargas convencionais.

6.8.2. Para suportar *racks* com até 65 kW, a solução deverá empregar arquitetura de resfriamento híbrida, combinando tecnologias de ***air cooling*** e preparação para ***liquid cooling***, de modo a atender à demanda atual e preservar capacidade de evolução futura.

6.8.3. Inicialmente, a climatização do POD de IA deverá utilizar combinação de ***Rear Door Heat Exchangers*** **(RDHx**) e equipamentos ***In-Row***, permitindo retirar a maior parcela da carga térmica diretamente na parte traseira dos *racks* e tratar a carga remanescente por meio de climatização de precisão entre *racks*.

6.8.4. Essa composição é necessária porque os RDHx atuam diretamente na fonte de geração de calor, reduzindo a descarga térmica para o ambiente e permitindo a operação de *racks* de maior densidade. O *In-Row* , por sua vez, complementa a capacidade térmica, contribui para o controle do corredor técnico e garante estabilidade ambiental ao POD.

6.8.5. A solução também deverá permitir futura migração parcial ou total para *liquid cooling*, com alterações mínimas na infraestrutura, considerando que o mercado de servidores de IA está em rápida evolução e que determinadas gerações de equipamentos podem exigir ou recomendar resfriamento líquido direto.

6.8.6. A adoção de infraestrutura preparada para *liquid cooling* evita obsolescência precoce, reduz riscos de retrabalho, preserva o investimento público e permite que a Administração acompanhe a evolução tecnológica dos servidores de IA sem necessidade de reconstrução integral da infraestrutura de climatização.

6.9. Necessidade de *chillers indoor*, CDU e simplificação hidráulica:

6.9.1. A solução de climatização deverá utilizar *chillers* do tipo *indoor*, com condensação externa, de forma a reduzir o peso dos equipamentos instalados na laje técnica, que possui limitação estrutural estimada em 150 kg /m².

6.9.2. Essa escolha tecnológica é necessária porque equipamentos *outdoor* completos poderiam impor peso e esforços superiores aos mais adequados à infraestrutura existente. Ao utilizar *chillers indoor*, concentra-se a maior parte dos componentes em ambiente interno controlado, deixando na laje apenas os elementos de condensação compatíveis com a capacidade estrutural disponível.

6.9.3. Além disso, a utilização de *chillers indoor* favorece a integração com CDU ou unidades equivalentes de distribuição de fluido, permitindo que a solução inicialmente destinada aos RDHx possa ser adaptada, com menor intervenção, para *racks* com *liquid cooling* no futuro.

6.9.4. Não se recomenda, para esta solução, a adoção de central de água gelada tradicional de grande porte, com tanque de termoacumulação, extensa rede hidráulica, grande quantidade de válvulas e múltiplos pontos de manutenção. Tal alternativa aumentaria a complexidade operacional, elevaria a dependência de manutenção especializada, ampliaria os pontos potenciais de falha e traria maior sensibilidade a problemas relacionados à disponibilidade e ao manejo de água no sítio.

6.9.5. A arquitetura escolhida deverá simplificar a operação hidráulica, reduzir pontos de falha, melhorar a manutenibilidade e facilitar a futura migração para *liquid cooling*, sem comprometer a capacidade de resfriamento do POD de IA.

6.10. Necessidade de *continuous cooling* para o POD de IA:

6.10.1. A alta densidade térmica do POD de IA torna indispensável a continuidade do resfriamento durante eventos de transição elétrica, especialmente no intervalo entre a interrupção da alimentação principal e a entrada estabilizada dos grupos geradores.

6.10.2. Em ambientes convencionais, a inércia térmica pode ser suficiente para suportar pequenos intervalos sem climatização plena. Todavia, em *racks* de IA com até 65 kW, a elevação de temperatura pode ocorrer rapidamente, gerando risco de *hotspots*, desligamento de equipamentos, degradação de desempenho, perda de processamento e indisponibilidade de sistemas críticos.

6.10.3. Por essa razão, a solução deverá prever UPS dedicado à climatização, com capacidade dimensionada para manter o resfriamento do POD de IA durante o período necessário à partida, transferência e estabilização dos geradores.

6.10.4. Essa abordagem substitui a necessidade de tanque de termoacumulação como *buffer* térmico principal, reduzindo complexidade hidráulica, espaço ocupado, manutenção e riscos associados a reservatórios, bombas, válvulas e grandes volumes de água gelada.

6.10.5. O *continuous cooling* por meio de UPS dedicado à climatização representa, portanto, uma solução mais simplificada, eficiente e aderente à realidade do DC RF, garantindo proteção térmica contínua ao POD de IA e reduzindo riscos operacionais.

6.11. Necessidade de eficiência energética:

6.11.1. A expansão do DC RF para processamento de IA elevará significativamente a demanda energética do ambiente. Por essa razão, a solução tecnológica deverá incorporar medidas de eficiência energética, especialmente nos sistemas de climatização e distribuição elétrica.

6.11.2. Os *chillers* deverão empregar tecnologia de ***free cooling***, permitindo aproveitamento de condições ambientais favoráveis para reduzir o uso de compressão mecânica e, consequentemente, diminuir o consumo energético ao longo do ciclo de vida da solução.

6.11.3. Também deverão ser adotadas soluções de distribuição elétrica compatíveis com alta densidade, como barramento blindado aéreo, UPS modular, monitoramento de carga, setorização de circuitos e capacidade de expansão, de modo a permitir maior eficiência, flexibilidade e controle operacional.

6.11.4. A eficiência energética é requisito tecnológico essencial porque impacta diretamente o custo total de propriedade, a sustentabilidade da operação, a autonomia do sistema de geração, a capacidade de climatização e a viabilidade econômica da infraestrutura de IA no médio e longo prazo.

6.12. Necessidade de conectividade, cabeamento e redes de alta performance:

6.12.1. O processamento de IA, especialmente em ambientes com múltiplas GPUs e múltiplos servidores, depende de redes de alta velocidade, baixa latência e elevada largura de banda para comunicação entre nós computacionais, armazenamento e serviços de apoio.

6.12.2. A infraestrutura deverá prever cabeamento estruturado de alta densidade, rotas adequadas sob piso elevado ou por eletrocalhas, segregação entre cabeamento lógico e elétrico, identificação, organização e capacidade de crescimento.

6.12.3. Os 2 *racks* de Telecom previstos no POD de IA deverão concentrar equipamentos de rede, interconexão e distribuição necessários ao funcionamento do *cluster*, devendo ser dimensionados para suportar tráfego intenso, baixa latência e integração segura com a rede do DC RF.

6.12.4. A necessidade tecnológica de conectividade não se limita ao acesso externo dos sistemas, mas envolve, principalmente, a comunicação interna de alta performance entre servidores, GPUs, *storages*, *switches* e plataformas de orquestração de *workloads* de IA.

6.13. Necessidade de segurança, monitoramento e governança operacional:

6.13.1. Considerando a natureza estratégica da infraestrutura pretendida, a nova Sala Segura deverá contar com controles de segurança física, lógica e operacional compatíveis com ambiente crítico de *data center*.

6.13.2. Deverão ser previstos controles de acesso, monitoramento ambiental, CFTV, detecção e combate a incêndio, sensores de temperatura e umidade, monitoramento de energia, alarmes, integração com sistemas de gestão e procedimentos de operação assistida.

6.13.3. A criticidade dos dados e das cargas de IA exige que o ambiente permita rastreabilidade, auditabilidade, controle de intervenções, gestão de incidentes e pronta resposta a falhas. Essa necessidade reforça a opção por infraestrutura própria, instalada no DC RF, sob governança direta do Exército Brasileiro.

6.13.4. A solução deverá ainda prever suporte técnico, manutenção preventiva e corretiva, sistema de registro de chamados e níveis mínimos de serviço, de forma a assegurar a continuidade da operação e a adequada gestão do ambiente após sua implantação.

6.13.5. A criticidade dos serviços a serem suportados exige que a solução seja projetada segundo critérios de alta disponibilidade, redundância, tolerância a falhas e capacidade de operação em condições adversas, evitando que falhas isoladas de componentes provoquem indisponibilidade dos serviços hospedados.

6.13.6. Tal necessidade encontra aderência à **Portaria GM-MD nº 4.360/2026**, que determina que as soluções de Inteligência Artificial de Defesa sejam submetidas a requisitos adequados de segurança, proteção, eficácia e resiliência, incluindo **tolerância a falhas e degradação controlada**, de forma a assegurar operação segura mesmo em condições adversas ou sob ataque durante todas as fases de seu ciclo de vida.

6.13.7. Consequentemente, os requisitos de redundância de alimentação elétrica, UPS, grupos geradores, climatização, conectividade, monitoramento e demais sistemas de infraestrutura não constituem elementos acessórios da solução, mas mecanismos essenciais à garantia da continuidade operacional e da resiliência dos serviços hospedados.

6.14. Necessidade de certificação, disponibilidade e manutenção concorrente:

6.14.1. A infraestrutura deverá ser concebida para atender aos critérios de alta disponibilidade compatíveis com certificação Tier III, abrangendo projeto, implantação, comissionamento e validação da instalação.

6.14.2. A necessidade de certificação decorre da criticidade dos serviços prestados pelo DC RF e da necessidade de garantir que a expansão seja projetada e executada com padrões reconhecidos de resiliência, redundância e manutenção concorrente, bem como manter os já existenstes.

6.14.3. Para isso, os sistemas de energia, climatização, telecomunicações, segurança, automação e monitoramento deverão ser concebidos de forma integrada, evitando pontos únicos de falha que comprometam a continuidade da operação.

6.14.4. A exigência de certificação e comissionamento integrado também se justifica pela necessidade de assegurar que os diversos subsistemas funcionem como solução única, e não como componentes isolados sem validação conjunta.

6.14.5. Outro aspecto relevante para a definição da solução é a necessidade de preservação da autonomia tecnológica e da soberania sobre a infraestrutura destinada ao processamento e armazenamento de informações institucionais.

6.14.6. A Portaria GM-MD nº 4.360/2026, em seu art. 5º, estabelece como diretriz a obtenção de capacidades autóctones capazes de garantir autonomia estratégica e soberania tecnológica, incluindo a capacidade de projetar, desenvolver, produzir, controlar e proteger a infraestrutura digital e os sistemas críticos de Inteligência Artificial próprios, reduzindo dependências externas e vulnerabilidades tecnológicas estratégicas.

6.14.7. A disponibilidade de infraestrutura própria, segura, resiliente e sob controle institucional contribui diretamente para esse objetivo, especialmente quando considerada a possibilidade de hospedagem de dados sensíveis, aplicações críticas, sistemas de apoio à decisão e futuras cargas computacionais relacionadas à Inteligência Artificial de Defesa.

6.15. Síntese das necessidades tecnológicas:

6.15.1. Em síntese, a demanda tecnológica identificada exige a implantação de infraestrutura própria, segura, escalável e de alta disponibilidade para processamento de IA, contemplando:

6.15.1.1. Sala Segura de aproximadamente 130 m²;

6.15.1.2. POD de IA com 12 *racks* de TI de alta densidade e 2 *racks* de Telecom;

6.15.1.3. Capacidade para *racks* de até 65 kW;

6.15.1.4. Infraestrutura compatível com AI PODs de processamento massivo, especialmente classe GG;

6.15.1.5. Suporte a servidores acelerados por GPUs de alta performance;

6.15.1.6. Energia crítica com geração redundante em configuração N+1;

6.15.1.7. UPS modular para carga de TI;

6.15.1.8. UPS dedicado para climatização e *continuous cooling*;

6.15.1.9. Climatização híbrida com RDHx e *In-Row*;

6.15.1.10. *Chillers indoor* com condensação externa e tecnologia *free cooling*;

6.15.1.11. Preparação para migração futura para *liquid cooling*;

6.15.1.12. Distribuição elétrica flexível por barramento blindado;

6.15.1.13. Cabeamento estruturado de alta densidade;

6.15.1.14. *Racks* de Telecom para interconexão de alta performance;

6.15.1.15. Controle de acesso, monitoramento ambiental e segurança física;

6.15.1.16. Detecção e combate a incêndio;

6.15.1.17. Suporte técnico, manutenção e gestão de chamados; e

6.15.1.18. Projeto e implantação compatíveis com certificação Tier III.

6.15.2. Tais necessidades tecnológicas demonstram que a contratação deve ser orientada à implantação de uma solução integrada de infraestrutura crítica, e não à aquisição isolada de equipamentos. O objetivo é criar uma base permanente para processamento de IA no DC RF, com segurança, disponibilidade, eficiência energética, capacidade de expansão e aderência às demandas estratégicas do Exército Brasileiro.

6.16. Consolidação da justificativa da necessidade da contratação

6.16.1. Em atendimento ao art. 15 da Instrução Normativa SGD/ME nº 94/2022, a necessidade da presente contratação encontra-se fundamentada a partir do alinhamento entre a demanda institucional, os instrumentos de planejamento, o dimensionamento da infraestrutura necessária e os resultados pretendidos, conforme consolidado nos subitens seguintes.

6.16.2. Alinhamento da solução de TIC aos instrumentos de planejamento. A contratação encontra-se prevista no Plano de Contratações Anual de 2026, sob o ID PCA no PNCP nº 00394452000103-0-000296 /2026, item nº 360, identificador da futura contratação 160749-40/2026. Encontra-se, ainda, alinhada à Estratégia de Governo Digital, ao Plano Estratégico do Exército 2024-2027, ao Plano Estratégico de Tecnologia da Informação do Exército Brasileiro 2024-2027 e ao Plano Diretor de Tecnologia da Informação e Comunicação 2026-2027 do 7º CTA. Em especial, a contratação contribui para a centralização da hospedagem de sistemas, para o aperfeiçoamento da infraestrutura de TIC, para a implantação de novas capacidades de Comando, Controle e Informação e para a expansão e modernização do Data Center Coronel Ricardo Franco.

6.16.3. Relação entre a necessidade da contratação e os volumes e características do objeto. A necessidade administrativa decorre da insuficiência da infraestrutura atualmente disponível no Data Center Coronel Ricardo Franco para absorver, de forma segura, resiliente e escalável, o crescimento das cargas computacionais, especialmente aquelas associadas ao processamento de Inteligência Artificial. O dimensionamento da solução considera um ambiente de alta densidade composto por 12 racks de TI de até 65 kVA por rack, correspondendo a aproximadamente 780 kVA de carga crítica de TI, adotando-se capacidade de planejamento de até 800 kVA, além da previsão de 2 PODs padrão, destinados a cargas convencionais e futuras de TIC.

6.16.4. As características da solução decorrem diretamente dessas necessidades, abrangendo, de forma integrada, sala segura, infraestrutura elétrica, sistemas UPS, geração de energia, climatização de precisão, racks de alta densidade, cabeamento, monitoramento, segurança física, controle de acesso, combate a incêndio, movimentação de ativos, comissionamento, documentação, recertificação Tier III e suporte técnico, necessários à operação conjunta do ambiente.

6.16.5. Forma de cálculo e dimensionamento dos quantitativos. Os quantitativos da contratação foram definidos a partir do dimensionamento técnico desenvolvido no item 8 deste ETP, considerando a demanda atual identificada, a evolução tecnológica dos equipamentos destinados ao processamento de IA, a necessidade de atendimento das cargas computacionais previstas e horizonte de utilização de, no mínimo, 10 anos, com possibilidade de expansão.

6.16.6. Para o POD de IA, adotou-se como referência a instalação de 12 racks de alta densidade de 65 kVA, resultando em aproximadamente 780 kVA, arredondados para capacidade de planejamento de 800 kVA. Para os 2 PODs padrão, considerou-se carga de 165 kW por POD, resultando em acréscimo de aproximadamente 330 kW, de modo que a nova carga de TI considerada no dimensionamento alcança aproximadamente 1.130 kW.

6.16.7. A partir dessas cargas foram dimensionados os subsistemas correlatos. A infraestrutura elétrica considera a instalação de transformadores adicionais; os sistemas UPS foram dimensionados em função das cargas críticas de TI e climatização; e o sistema de geração considera a integração de 2 novos grupos motogeradores de 1 MVA aos 2 existentes, formando configuração redundante compatível com os requisitos de disponibilidade do ambiente. O dimensionamento dos demais componentes decorre da arquitetura integrada da solução, estando os quantitativos consolidados no item 8.7 deste ETP e detalhados no Termo de Referência e em suas especificações técnicas.

6.16.8. Resultados e benefícios a serem alcançados. A contratação tem como resultados esperados a expansão da capacidade institucional de hospedagem, processamento e sustentação dos sistemas estratégicos do Exército Brasileiro; a disponibilização de capacidade permanente para processamento de cargas intensivas de IA; o fortalecimento da soberania dos dados e da autonomia tecnológica; a redução da dependência de infraestrutura externa; a manutenção da disponibilidade e continuidade dos serviços críticos; a ampliação da segurança física e lógica dos ativos; o aumento da escalabilidade e da capacidade de absorção de futuras demandas; e a melhoria da eficiência operacional e energética da infraestrutura.

6.16.9. A solução também permitirá consolidar o Data Center Coronel Ricardo Franco como infraestrutura central de hospedagem e processamento do SisTEx, proporcionando ambiente próprio, controlado, seguro, resiliente e tecnologicamente evolutivo, apto a suportar tanto soluções de Inteligência Artificial quanto sistemas corporativos e demais cargas críticas da Força.

6.16.10. Adesão por órgãos ou entidades não participantes. Embora a contratação seja processada mediante Sistema de Registro de Preços, não será permitida a participação ou adesão de outros órgãos ou entidades à Ata de Registro de Preços, razão pela qual não há motivação para autorização de adesões por órgãos ou entidades não participantes. A restrição decorre das características específicas da solução, dimensionada para atendimento ao Data Center Corporativo do Exército Brasileiro em Brasília e compatibilizada com as condições físicas, elétricas, térmicas, operacionais e de infraestrutura existentes no Data Center Coronel Ricardo Franco.

7. Demais requisitos necessários e suficientes à escolha da solução de TIC

7.1. Requisitos Legais (Normas Técnicas):

7.1.1. Para garantir que o objeto seja cumprido com a capacidade desejada, é necessário que o projeto atenda às normas que se empregam também em projetos com equipamentos de TI.

7.1.2. O projeto e todos os componentes e procedimentos que serão utilizados na implementação da solução deverão, sempre que aplicável, estar em conformidade com todas as normas técnicas aplicáveis da ABNT e instituições internacionais, estando alinhados com, pelo menos, as seguintes normas:

7.1.2.1. ABNT NBR 10636-1:2022 - Paredes divisórias sem função estrutural - Determinação da resistência ao fogo.

7.1.2.2. NBR 5628 - Componentes construtivos estruturais.

7.1.2.3. ANSI/BICSI-002-2024 - *Datacenter Design and Implementation Best Practices*.

7.1.2.4. ABNT NBR 5471 - Condutores elétricos.

7.1.2.5. ABNT NBR 9442 - Materiais de construção - Determinação do índice de propagação superficial de chama pelo método do painel radiante - Método de ensaio.

7.1.2.6. ABNT NBR 10151 - Acústica - Avaliação do ruído em áreas habitadas, visando o conforto da comunidade.

7.1.2.7. ABNT NBR 10898:2023 - Sistema de iluminação de emergência.

7.1.2.8. NBR IEC 60529 - Grau de proteção providos invólucros.

7.1.2.9. ANSI-BICSI-009-2024 - *Datacenter Design and Implementation best Practices*. ANSI-BICSI-009-2019 - *Datacenter Operation and Maintenance best Practices*.

7.1.2.10. ABNT NBR 11802 - Pisos elevados - Especificação.

7.1.2.11. ABNT NBR 14565 - Cabeamento estruturado para edifícios comerciais e *Datacenters*.

7.1.2.12. ABNT NBR 15014 - Sistemas de alimentação de potência ininterrupta (*nobreaks*) *online*, interativo e *stand-by*, que utilizam bateria como fonte de energia armazenada.

7.1.2.13. ABNT NBR 17240 - Sistemas de detecção e alarme de incêndio - Projeto, instalação, comissionamento e manutenção de sistemas de detecção e alarme de incêndio.

7.1.2.14. ABNT NBR 5410 - Instalações elétricas de baixa tensão.

7.1.2.15. ABNT NBR 5419 - Proteção de estruturas contra Descargas Atmosféricas.

7.1.2.16. ABNT NBR 6492 - Representação de projetos de arquitetura.

7.1.2.17. ABNT NBR IEC 60947-2 - Dispositivos de manobra e comando de baixa tensão.

7.1.2.18. ABNT NBR ISO 7240-1 - Sistemas de detecção e alarme de incêndio Parte 1: Generalidades e definições.

7.1.2.19. ABNT NBR ISO/IEC 27001 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.

7.1.2.20. ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação.

7.1.2.21. ABNT NBR 14039: Necessária para a "Subestação Interna" e entrada de energia.

7.1.2.22. ABNT NBR 15247: Norma específica para Salas Seguras, e quando não couber a ISO/IEC 22237.

7.1.2.23. ABNT NR 16401-1:2024 - Instalações de ar-condicionado - Sistemas centrais e unitários - Parte 1: Projetos das instalações.

7.1.2.24. ABNT NR 16401-2:2024 - Instalações de ar-condicionado - Sistemas centrais e unitários - Parte 2: Parâmetros de conforto térmico.

7.1.2.25. ABNT NR 16401-3:2024 - Instalações de ar-condicionado - Sistemas centrais e unitários - Parte 3: Qualidade do ar interior.

7.1.2.26. ANSI/TIA-942-C (ou mais recente): norma de infraestrutura e para *design* de DC com redundância e resiliência (alinhada ao Tier III)

7.1.2.27. ANSI/TIA/EIA-569-E - *Commercial Building Standard for Telecommunications Pathways and Spaces*.

7.1.2.28. ANSI/TIA-606-D:2021 - *Administration Standard for Telecommunications Infrastructure*.

7.1.2.29. ASHRAE TC 9.9 (*Thermal Guidelines for Data Processing Environments*): para resfriamento de equipamentos de alta densidade e define os limites de temperatura e umidade necessários para GPUs modernas.

7.1.2.30. ASTM A106/ A106M - *Standard Specification for Seamless Carbon Steel Pipe for High-Temperature Service*.

7.1.2.31. ASTM E119-12 - *Standard Test Methods for Fire Tests of Building Construction and Materials*.

7.1.2.32. ASTM E662 - *Standard Test Method for Specific Optical Density of Smoke Generated by Solid Materials*.

7.1.2.33. BS EN 50173-5:2007+A1 - *Information technology. Generic cabling systems. Data Centers*.

7.1.2.34. ISO 1182 - *Reaction to fire tests for products - Non-combustibility test*.

7.1.2.35. ISO/IEC-11801 - *Information Technology - Generic Cabling for Customer Premisses*.

7.1.2.36. ISO/IEC 30134 (Série): Indicadores de eficiência energética, como o PUE (*Power Usage Effectiveness*).

7.1.2.37. MTE/NR n° 01 - Segurança do Trabalho: Disposições Gerais.

7.1.2.38. MTE/NR n° 04 - Serviços Especializados em Engenharia de Segurança e em Medicina do Trabalho.

7.1.2.39. MTE/NR n° 06 - Equipamentos de Proteção Individual (EPI).

7.1.2.40. MTE/NR n° 10 - Segurança em Instalações e Serviços em Eletricidade.

7.1.2.41. MTE/NR n° 11 - Transporte, Movimentação, Armazenagem e Manuseio de Materiais.

7.1.2.42. MTE/NR n° 12 - Segurança no Trabalho em Máquinas e Equipamentos. MTE/NR N°17 - Ergonomia.

7.1.2.43. MTE/NR n° 23 - Proteção Contra Incêndios. MTE/NR n° 26 - Sinalização de Segurança.

7.1.2.44. MTE/NR n° 28 - Fiscalização e Penalidades.

7.1.2.45. NFPA-2001 - *Standard on Clean Agent Fire Extinguishing Systems*.

7.1.2.46. NFPA-75 - *Standard for the Fire Protection of Information Technology Equipment*.

7.1.3. As normas técnicas relacionadas no item 7.1.2 serão exigíveis exclusivamente em relação aos componentes, sistemas, materiais, procedimentos e atividades compreendidos em seus respectivos campos de aplicação e efetivamente integrantes do objeto contratado, não devendo sua indicação ser interpretada como imposição de requisito estranho ao objeto ou de certificação da licitante ou da CONTRATADA, salvo quando tal certificação estiver expressamente prevista neste ETP, no Termo de Referência ou em suas especificações técnicas.

7.1.3.1. Quando duas ou mais normas relacionadas estabelecerem critérios equivalentes para o mesmo requisito técnico, sua aplicação não será cumulativa quando isso resultar em duplicidade de ensaios, certificações ou comprovações, admitindo-se o atendimento pela norma expressamente indicada para o respectivo componente ou por equivalente tecnicamente aceita pela Administração, quando assim previsto no instrumento convocatório.

7.1.4. As normas nacionais poderão ser substituídas por normas internacionais desde que cumpram os requisitos mínimos previstos nas normas correspondentes ou que sejam amplamente reconhecidas e utilizadas nas melhores práticas de implantação, operação e manutenção de *data center*.

7.1.5. Quaisquer especificações técnicas constantes no Estudo Técnico Preliminar e Termo de Referência que, porventura, apresentem divergência com normas técnicas, legais ou regulamentares vigentes deverão ser interpretadas em conformidade com essas normas, prevalecendo sempre suas disposições. A contratada deverá considerar e assumir integralmente tais condições já no ato de elaboração de sua proposta.

7.1.6. O CONTRATANTE poderá solicitar, a qualquer tempo, comprovação normativa de aderência dos componentes e procedimentos utilizados na solução.

7.2. Requisitos de Garantia Técnica, Suporte e Manutenção:

7.2.1. Considerando a natureza crítica da solução a ser contratada, destinada à expansão das capacidades operacionais do *Data Center* Coronel Ricardo Franco, deverão ser previstos requisitos mínimos de garantia, suporte técnico especializado e manutenção preventiva e corretiva, de modo a assegurar a continuidade operacional, a disponibilidade dos serviços, a preservação dos investimentos realizados e a rápida recomposição do ambiente em caso de falhas.

7.2.2. A solução deverá contar com garantia mínima de 12 (doze) meses, complementar à garantia legal, contada a partir do recebimento definitivo do objeto, abrangendo os serviços executados, os equipamentos fornecidos, a integração entre os subsistemas e a correção de falhas decorrentes da implantação. Tal exigência

se justifica pelo caráter integrado da contratação, que envolve sala segura, energia crítica, UPS, grupos geradores, climatização de precisão, *chillers*, *rear door heat exchangers*, *in-row cooling*, barramentos, cabeamento, sistemas de segurança, automação, monitoramento e demais componentes de infraestrutura crítica.

7.2.3. Durante o período de garantia, a contratada deverá assegurar suporte técnico especializado e manutenção corretiva e preventiva, incluindo mão de obra, peças, componentes, transporte, seguros, deslocamento, estadia de técnicos e demais custos necessários à plena recomposição da solução, sem ônus adicional para a Administração. Essa exigência é necessária para evitar que falhas em equipamentos ou subsistemas críticos gerem custos imprevistos ao Contratante ou comprometam a continuidade dos serviços prestados pelo *Data Center*.

7.2.4. Considerando que o ambiente a ser implantado suportará cargas críticas e de alta densidade, especialmente associadas ao processamento de Inteligência Artificial, o suporte técnico deverá estar disponível em regime 24x7, com canais múltiplos para abertura de chamados, tais como telefone, e-mail e sistema *web*. A exigência de atendimento contínuo decorre da necessidade de pronta resposta a incidentes que possam afetar energia, climatização, segurança física, conectividade, disponibilidade dos racks ou operação dos sistemas hospedados.

7.2.5. Também deverá ser prevista ferramenta *web* para registro, acompanhamento e emissão de relatórios dos chamados técnicos, permitindo rastreabilidade, controle de prazos, identificação dos equipamentos afetados, histórico de intervenções, comprovação das soluções aplicadas e fiscalização dos níveis de serviço. Essa medida contribui para a governança contratual, para a transparência da execução e para a gestão de riscos operacionais.

7.2.6. Os níveis mínimos de atendimento deverão ser definidos no Termo de Referência de acordo com a severidade dos incidentes, distinguindo, no mínimo, ocorrências críticas, urgentes e de rotina. Os incidentes críticos deverão receber tratamento prioritário, especialmente quando puderem tornar inoperantes sistemas corporativos ou comprometer a infraestrutura essencial do *data center*. Os prazos, penalidades, indicadores de atendimento, critérios de medição e eventuais descontos decorrentes de descumprimento dos níveis de serviço deverão ser detalhados no Termo de Referência e nos seus apêndices.

7.2.7. A manutenção preventiva programada também deverá integrar a solução, com periodicidade e escopo definidos no Termo de Referência, abrangendo os principais sistemas que compõem o ambiente crítico. A manutenção preventiva é necessária para reduzir a probabilidade de falhas, preservar a vida útil dos equipamentos, manter a eficiência energética, assegurar a operação adequada dos sistemas de energia e climatização e apoiar a manutenção das condições necessárias à certificação e à alta disponibilidade do *data center*.

7.2.8. Dessa forma, a previsão de garantia mínima, suporte técnico 24x7, manutenção preventiva e corretiva, sistema de gestão de chamados e níveis mínimos de serviço constitui requisito necessário e suficiente à escolha da solução de TIC, pois está diretamente relacionada à mitigação de riscos, à continuidade operacional, à proteção do investimento público e à disponibilidade dos serviços críticos hospedados no *data center*.

7.3. Requisitos Temporais:

7.3.1. Os serviços devem ser prestados no **prazo máximo de 390 (trezentos e noventa) dias corridos**, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pelo CONTRATANTE, podendo ser prorrogada, excepcionalmente, por até 150 (cento e cinquenta) dias corridos, desde que justificado previamente pela CONTRATADA e autorizado pelo CONTRATANTE.

7.3.2. Quando não expressados de forma contrária a contagem dos prazos estabelecidos será considerada em dias corridos e excluir-se-á o dia do início e incluir-se-á o do vencimento.

7.3.3. Na execução dos serviços de expansão do DC RF, observa-se os **prazos** indicados na tabela a seguir:

FASE	ID	EVENTO	ETAPA	DIAS CORRIDOS	TEMPO ACUMULADO
Projetos básico e executivo	1.1	Reunião e assinatura do contrato	Assinatura do contrato	0	0
	1.1	Reunião e assinatura do contrato	Reunião inicial	5	5
	1.2	Entrega e aprovação dos projetos	Início dos projetos básico e executivo	5	10
	1.2	Entrega e aprovação dos projetos	Envio da primeira versão dos projetos	60	70
	1.2	Entrega e aprovação dos projetos	Análise dos projetos e eventuais correções	10	80
	1.2	Entrega e aprovação dos projetos	Aprovação dos projetos	15	95
	1.3	Recertificação TIER III	**Recertificação *Uptime Institute* TIER III *Design***	60	155
	2.1	Adaptações civis	Montagem do canteiro de serviços	20	175
	2.1	Adaptações civis	Conclusão da reforma civil interna	15	190
	2.1	Adaptações civis	Conclusão do *radier* condensadoras e *chiller*	10	200
	2.2	Sala Segura	Montagem da sala segura	15	215
	2.3	Entrega de GMG, UPS e *racks*	Entrega dos *racks* SIIA	8	223
	2.3	Entrega de GMG, UPS e *racks*	Entrega dos *racks* EDA	5	228
	2.3	Entrega de GMG, UPS e *racks*	Entrega dos *nobreaks*	7	235

Execução das instalações físicas	2.3	Entrega de GMG, UPS e *racks*	Entrega dos quadros elétricos	8	243
	2.3	Entrega de GMG, UPS e *racks*	Entrega dos geradores	7	250
	2.4	Entrega de Climatização, CFTV, Sensores e Cabos	Entrega dos cabos elétricos (ramal alimentador)	5	255
	2.4	Entrega de Climatização, CFTV, Sensores e Cabos	Entrega das máquinas de ar condicionado de precisão e *chiller*	5	260
	2.4	Entrega de Climatização, CFTV, Sensores e Cabos	Entrega dos materiais de Monitoramento (SDCI, DCIM e Seg. Organica)	5	265
	2.4	Entrega de Climatização, CFTV, Sensores e Cabos	Entrega dos materiais de cross connect metálico	5	270
	2.4	Entrega de Climatização, CFTV, Sensores e Cabos	Entrega dos materiais de *Cross Connect* ótico	5	275
	2.5	Instalação Climatização, GMG, UPS, Ramais, Sensores e Cabos	Montagem dos *racks* e confinamento	4	279
	2.5	Instalação Climatização, GMG, UPS, Ramais, Sensores e Cabos	Montagem dos quadros elétricos	10	289
	2.5	Instalação Climatização, GMG, UPS, Ramais, Sensores e Cabos	Montagem dos *nobreaks*	4	293
	2.5	Instalação Climatização, GMG, UPS, Ramais, Sensores e Cabos	Montagem das linhas frigoríferas	14	307
	2.5	Instalação Climatização, GMG, UPS, Ramais, Sensores e Cabos	Término do lançamento do ramal alimentador	5	312

	2.5	Instalação Climatização, GMG, UPS, Ramais, Sensores e Cabos	Término da montagem do *cross connect* metálico	3	315
	2.6	*Start up* GMG e Subestação	*Start up* dos geradores	15	330
	2.6	*Start up* GMG e Subestação	*Start up* da Subestação	15	345
	2.7	Expansão do Monitoramento e Comissionamento	Expansão do Sistema de segurança e monitoramento (SDCI, DCIM e Seg. Orgânica)	5	350
	2.7	Expansão do Monitoramento e Comissionamento	Execução dos testes e comissionamento	5	355
Recertificação TIER III	3.1	Recertificação TIER III	Recertificação *Uptime Institute* TIER III *Facilities*	10	365
Moving	4.1	Execução do moving	Entrega do planejamento do *moving*	10	375
	4.1	Execução do moving	Execução do *moving*	15	**390**
As Built	5.1	Entrega do As Built	Entrega do *As Built*	10	400
Garantia	6.1	Garantia	Garantia	365	765

7.4. Análise quanto a contratação em grupo:

7.4.1. A solução compõe-se de itens interdependentes e interoperáveis entre si, e considerando ainda que problemas na implantação de qualquer um dos itens pode comprometer o funcionamento dos demais, e por consequência da solução como um todo, comprometendo os rsultados do projeto, verifica-se a necessidade de realizar o certame licitatório em grupo único, conforme detalhamento constante em item específico deste ETP.

7.4.2. A opção pela contratação em grupo único também influencia a análise da margem de preferência, uma vez que a solução é composta por bens e serviços heterogêneos, interdependentes e integrados, não correspondendo a um único produto manufaturado nacional sujeito à aplicação da margem. Assim, eventual margem de preferência aplicável a componente isolado não autoriza sua incidência sobre o objeto global da contratação.

7.5. Análise quanto à aplicação de margem de preferência:

7.5.1. Foi avaliada a eventual incidência de margem de preferência prevista no art. 26 da Lei nº 14.133/2021, regulamentada, no âmbito federal, pelo Decreto nº 11.890/ 2024 e pelas resoluções da Comissão Interministerial de Contratações Públicas para o Desenvolvimento Sustentável - CICS.

7.5.2. A contratação pretendida, todavia, possui natureza de solução integrada para expansão de *data center*, abrangendo fornecimento de equipamentos, serviços especializados, instalação, integração, comissionamento, certificação, suporte técnico e adequações de infraestrutura crítica. Assim, o objeto global não corresponde a um único produto manufaturado nacional sujeito à margem de preferência.

7.5.3. Além disso, a contratação será estruturada em grupo único, em razão da interdependência técnica entre os subsistemas de energia, climatização, segurança, *racks*, cabeamento, monitoramento e certificação. Considerando que a solução é composta por bens e serviços heterogêneos, inclusive itens não enquadrados nas listas da CICS, não se mostra aplicável a margem de preferência ao grupo como um todo.

7.5.4. Ressalva-se que determinados componentes isolados da solução poderão, em tese, corresponder a produtos manufaturados nacionais constantes das resoluções vigentes da CICS. Contudo, a aplicação da margem de preferência exige identificação específica do NCM, comprovação da regra de origem ou qualificação e compatibilidade com a forma de julgamento da licitação. Dessa forma, para a presente contratação integrada, não será prevista margem de preferência, sem prejuízo da observância das normas aplicáveis caso algum item venha a ser contratado de forma autônoma em procedimento específico.

7.6. Requisitos de implantação da solução:

7.6.1. Considerando que a solução pretendida envolve a expansão de infraestrutura crítica de *data center*, com integração entre Sala Segura, energia, climatização, telecomunicações, segurança, monitoramento, *racks*, cabeamento, sistemas de proteção e demais subsistemas, a contratação deverá contemplar a entrega integrada da solução, incluindo fornecimento, montagem, instalação, configuração, integração, ligação inicial, testes, comissionamento, certificações e treinamento.

7.6.2. A exigência de implantação integrada se justifica pela interdependência técnica entre os subsistemas. Falhas de compatibilização entre energia, climatização, cabeamento, segurança física, automação, controle de acesso e infraestrutura da Sala Segura podem comprometer a disponibilidade, a certificação, a segurança e a operação do *data center*. Dessa forma, a solução não deve ser tratada como simples fornecimento isolado de equipamentos, mas como implantação de ambiente crítico em regime de responsabilidade integrada.

7.6.3. A contratada deverá apresentar os projetos necessários à implantação, incluindo projetos executivos, diagramas, *layouts*, esquemas de cabeamento, projetos elétricos, civis, lógicos, de climatização, segurança e demais documentos técnicos indispensáveis à execução e validação da solução.

7.6.4. A implantação deverá considerar a continuidade operacional do 7º CTA, de modo que atividades com potencial de impacto sobre a rotina do órgão ou sobre os serviços atualmente hospedados no *Data Center* sejam previamente planejadas, programadas e executadas em janelas acordadas com a Administração.

7.6.5. A movimentação de equipamentos existentes, quando necessária, deverá ser tratada como atividade crítica, planejada e controlada, considerando riscos de indisponibilidade, necessidade de preservação dos ativos, integridade das conexões, continuidade dos serviços, segurança física e rastreabilidade das intervenções.

7.6.6. Assim, a exigência de implantação coordenada e integrada constitui requisito necessário à escolha da solução de TIC, pois reduz riscos de incompatibilidade, evita fragmentação de responsabilidade e assegura que a solução seja entregue como ambiente operacional completo.

7.7. Requisitos de segurança da informação e privacidade:

7.7.1. Considerando a natureza crítica e sensível da infraestrutura a ser implantada, a solução deverá observar os princípios e procedimentos da Política de Segurança da Informação do Contratante, bem como os controles internos aplicáveis à proteção de dados, configurações, topologias, credenciais, parâmetros de rede e demais informações técnicas obtidas durante a execução contratual.

7.7.2. A contratada e os profissionais envolvidos na execução deverão manter sigilo sobre todas as informações acessadas em razão da contratação, sendo vedado o compartilhamento, a divulgação, a cópia ou a retenção de informações técnicas, configurações de ativos, dados operacionais, diagramas, registros ou quaisquer elementos da arquitetura do ambiente sem autorização expressa da Administração.

7.7.3. A exigência de assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS e Termo de Ciência pelos profissionais envolvidos se justifica em razão do acesso a ambiente crítico de *data center*, com informações potencialmente sensíveis sobre infraestrutura de TIC, segurança, redes, sistemas, ativos e arquitetura operacional do Exército Brasileiro.

7.7.4. Após concluídas as atividades de implantação, *moving*, configuração, testes ou suporte, a contratada deverá eliminar de seus meios próprios as informações técnicas que não sejam necessárias à garantia, ao suporte autorizado ou à documentação formal entregue à Administração, preservando-se a cadeia de custódia e a confidencialidade dos dados do Contratante.

7.7.5. Esses requisitos são necessários para mitigar riscos de vazamento de informações, engenharia social, exposição de topologia de rede, uso indevido de configurações, acesso não autorizado e comprometimento da segurança física e lógica do ambiente.

7.8. Requisitos de vistoria técnica:

7.8.1. Será assegurado aos interessados o direito de realização de vistoria técnica prévia, acompanhada por servidor designado, com a finalidade de permitir o conhecimento das condições locais, das peculiaridades do ambiente, das restrições de acesso, das interfaces com a infraestrutura existente e dos riscos associados à implantação da solução.

7.8.2. A vistoria deve ser tratada como **facultativa, porém recomendada**, considerando a complexidade do objeto e a necessidade de conhecimento prévio do ambiente de execução. A não realização da vistoria poderá ser substituída por declaração formal do responsável técnico da licitante de que possui pleno conhecimento das condições e peculiaridades da contratação.

7.8.3. A exigência de declaração formal em caso de não realização da vistoria se justifica para evitar alegações futuras de desconhecimento das instalações, das condições de acesso, das limitações físicas, das rotas de cabeamento, das interfaces com sistemas existentes e de outros elementos que possam impactar a execução.

7.8.4. Considerando a natureza sensível do ambiente, os profissionais que realizarem a vistoria deverão estar devidamente identificados e deverão assinar termo de sigilo, a fim de proteger informações técnicas, operacionais e de segurança eventualmente acessadas durante a visita.

7.8.5. O detalhamento de horários, procedimentos de agendamento, documentos exigidos, responsáveis pelo acompanhamento e modelo de termo deverá constar no Termo de Referência.

7.9. Requisitos de sustentabilidade:

7.9.1. A solução deverá observar critérios de sustentabilidade compatíveis com a natureza do objeto, com o Plano Diretor de Logística Sustentável do órgão e com o Guia Nacional de Contratações Sustentáveis, especialmente quanto à eficiência energética, destinação ambientalmente adequada de resíduos, logística reversa, descarte de componentes, redução de impactos ambientais e utilização de tecnologias compatíveis com boas práticas ambientais.

7.9.2. A contratada deverá ser responsável pela destinação adequada dos resíduos gerados durante a implantação, manutenção preventiva, manutenção corretiva, substituição de componentes, embalagens e demais atividades associadas à execução da solução.

7.9.3. A solução deverá vedar o fornecimento de produtos que contenham ou utilizem substâncias que destroem a camada de ozônio, quando proibidas pela legislação aplicável, especialmente CFCs, Halons, CTC e tricloroetano, ressalvadas apenas as hipóteses legalmente permitidas.

7.9.4. A exigência de sustentabilidade se justifica pela natureza permanente da solução, pelo consumo energético relevante de ambientes de *data center*, pela presença de equipamentos eletroeletrônicos, baterias, sistemas de climatização, componentes metálicos, cabos, embalagens e resíduos técnicos que demandam destinação ambientalmente adequada.

7.9.5. Tais requisitos contribuem para reduzir impactos ambientais, preservar recursos, assegurar conformidade regulatória e promover maior eficiência ao longo do ciclo de vida da solução.

7.9.6. Em atenção ao Plano Diretor de Logística Sustentável do 7º CTA deverão ser observados ainda os seguintes aspectos:

7.9.6.1. As soluções tecnológicas devem priorizar sistemas e equipamentos que exijam menor intensidade de manutenção preventiva e corretiva ao longo de seu ciclo de vida, de forma a reduzir os custos indiretos.

7.9.6.2. Adoção de infraestrutura preparada para *liquid cooling* de forma a evitar obsolescência precoce, reduzir riscos de retrabalho, preservar o investimento público e permitir que a Administração acompanhe a evolução tecnológica dos servidores de IA.

7.9.6.3. Considerar a demanda energética do novo ambiente, considerando medidas de eficiência energética, especialmente nos sistemas de climatização e distribuição elétrica.

7.10. Requisitos sociais, ambientais e culturais:

7.10.1. A documentação técnica, os manuais, os relatórios e os registros associados à execução, operação, suporte e manutenção da solução deverão ser fornecidos preferencialmente em língua portuguesa, ou acompanhados de documentação suficiente para compreensão e operação pela equipe técnica do Contratante.

7.10.2. A exigência se justifica pela necessidade de assegurar transferência de conhecimento, adequada operação assistida, manutenção básica, fiscalização contratual, rastreabilidade das intervenções e autonomia da equipe técnica do 7º CTA após a entrega da solução.

7.10.3. Os requisitos sociais, ambientais e culturais também abrangem a correta destinação de resíduos, a logística reversa, a observância de normas ambientais aplicáveis e a realização de capacitação em condições que permitam efetivo aprendizado pelos integrantes indicados pela Administração.

7.11. Requisitos de arquitetura tecnológica:

7.11.1. A solução deverá observar as diretrizes de arquitetura tecnológica estabelecidas pela área técnica do Contratante, de modo a assegurar compatibilidade com a infraestrutura existente, aderência aos padrões institucionais, integração com os sistemas legados e alinhamento às necessidades de alta disponibilidade do *data center*.

7.11.2. A adoção de arquitetura, tecnologia, componente ou solução diversa daquela aprovada deverá depender de autorização prévia do Contratante, considerando os riscos de incompatibilidade, perda de garantia, prejuízo de desempenho, aumento de complexidade operacional ou inviabilização da certificação pretendida.

7.11.3. Todos os componentes da solução deverão ser compatíveis entre si e deverão ter seu funcionamento integrado testado antes do recebimento definitivo. Essa exigência é essencial porque o ambiente de *data center* depende da atuação coordenada de sistemas elétricos, climatização, segurança física, cabeamento, racks, automação, controle de acesso, monitoramento e demais componentes.

7.11.4. A solução poderá ser composta por produtos de diferentes fabricantes, desde que a contratada garanta a integração, a interoperabilidade, a compatibilidade e o pleno funcionamento conjunto de todos os produtos e módulos entregues. A responsabilidade pela compatibilização técnica deverá permanecer integralmente com a contratada.

7.11.5. Os componentes ofertados não deverão estar em situação de fim de venda ou fim de vida útil pelo fabricante na data da proposta, a fim de evitar aquisição de tecnologia obsoleta, indisponibilidade de peças, restrição de suporte, dificuldade de manutenção e risco de descontinuidade operacional.

7.11.6. A solução deverá contemplar todos os equipamentos, *softwares*, licenças, acessórios e componentes necessários ao correto funcionamento do ambiente, evitando dependências não previstas, custos adicionais futuros ou lacunas de fornecimento. Quando houver licenciamento de *software* indispensável ao funcionamento da solução, deverá ser priorizado modelo que assegure continuidade de uso pela Administração, conforme condições estabelecidas no Termo de Referência.

7.11.7. Os requisitos de padronização de determinados componentes, como *racks*, confinamento, cabeamento metálico e cabeamento óptico, deverão ser tratados no Termo de Referência com justificativa técnica específica, considerando compatibilidade, garantia, desempenho, vedação de vazamento de ar frio, interoperabilidade e redução de riscos de falha.

7.12. Requisitos de proteção física da Sala Segura:

7.12.1. A solução deverá contemplar ambiente físico seguro, compatível com a criticidade dos ativos de TIC e das cargas de processamento de IA a serem hospedadas, incluindo elementos de proteção física, controle de acesso, monitoramento, compartimentação, proteção contra incêndio e demais recursos necessários à preservação da disponibilidade e da segurança do *data center*.

7.12.2. A Sala Segura deverá possuir elementos construtivos compatíveis com requisitos de estabilidade, estanqueidade e isolamento térmico, observadas as normas técnicas aplicáveis e os requisitos de proteção ao fogo definidos no Termo de Referência.

7.12.3. A proteção física do ambiente é requisito indispensável porque a solução hospedará equipamentos de alto valor, elevada criticidade operacional e alta densidade energética, cuja indisponibilidade ou dano pode afetar serviços corporativos e estratégicos.

7.12.4. Os requisitos detalhados de desempenho da Sala Segura, incluindo resistência ao fogo, certificações, características de paredes, piso, teto, portas, vedação, controle de acesso, CFTV e combate a incêndio, deverão ser especificados no Termo de Referência e em seus apêndices técnicos.

7.13. Requisitos de segurança física, privacidade, controle de acesso e videomonitoramento:

7.13.1. A solução deverá prever recursos de segurança física compatíveis com ambiente crítico de *data center*, contemplando controle de acesso, identificação de usuários, videomonitoramento, registro de eventos, monitoramento ambiental e integração com os procedimentos de segurança do Contratante.

7.13.2. A adoção de controle de acesso com múltiplos fatores, leitoras biométricas, cartões de identificação e câmeras IP com alimentação PoE, quando especificada no Termo de Referência, justifica-se pela necessidade de restringir o acesso ao ambiente, registrar eventos, facilitar auditorias e reduzir riscos de acesso indevido a ativos críticos.

7.13.3. Tais requisitos são necessários para preservar a segurança física dos equipamentos, a rastreabilidade das intervenções e a proteção das informações e sistemas hospedados.

7.14. Requisitos de experiência profissional e formação da equipe:

7.14.1. A implantação, manutenção, garantia e suporte da solução deverão ser realizados por profissionais devidamente capacitados, com experiência compatível com ambientes de *data center*, infraestrutura crítica, sistemas elétricos, climatização de precisão, cabeamento, segurança, automação, comissionamento e demais disciplinas pertinentes ao objeto.

7.14.2. A exigência de profissionais qualificados se justifica pela complexidade da solução, pelo risco de indisponibilidade dos serviços, pela necessidade de integração entre subsistemas e pela criticidade dos ativos envolvidos.

7.14.3. Os profissionais alocados deverão possuir conhecimentos, habilitações, credenciamentos e certificações compatíveis com as atividades que executarão, incluindo registro profissional em conselho competente, quando a natureza da atividade assim exigir.

7.14.4. A comprovação de experiência em atividade semelhante deverá ser exigida de forma proporcional ao objeto, sem restringir indevidamente a competitividade, mas assegurando que a equipe possua capacidade técnica para atuar em ambiente crítico e de alta disponibilidade.

7.15. Requisitos de metodologia de trabalho:

7.15.1. A execução dos serviços deverá observar metodologia formal de trabalho, com emissão de ordens de serviço, definição de escopo, cronograma, responsáveis, localidades de execução, critérios de aceitação, registros de acompanhamento e validação das entregas.

7.15.2. A adoção de metodologia estruturada se justifica pela necessidade de coordenar múltiplas disciplinas técnicas, reduzir riscos de retrabalho, preservar a continuidade operacional do 7º CTA, controlar interfaces com sistemas existentes e assegurar rastreabilidade das decisões técnicas.

7.15.3. Deverá ser realizada reunião inicial entre Contratante e Contratada, com apresentação do preposto, validação do cronograma, definição dos canais de comunicação, entrega dos termos de sigilo e alinhamento dos procedimentos de execução, fiscalização e aceitação.

7.15.4. A contratada deverá apresentar os projetos, planos e documentos necessários à execução, incluindo, quando aplicável, projetos civis, elétricos, lógicos, diagramas de blocos, *layout* do *data center*, esquemáticos de cabeamento, planos de instalação, planos de testes, planos de comissionamento e documentação final "*as built* ".

7.15.5. O Contratante será responsável pela gestão e fiscalização contratual, cabendo à contratada a execução técnica, a coordenação dos recursos humanos e materiais, a compatibilização das entregas e a garantia da conformidade da solução com os requisitos estabelecidos.

7.15.6. Os prazos específicos de início, execução, atendimento, etapas, marcos e entregas deverão ser definidos no Termo de Referência, de modo a permitir fiscalização objetiva e aplicação dos critérios de recebimento.

7.16. Requisitos de comunicação, registro de ocorrências e suporte:

7.16.1. A solução deverá prever meios formais de comunicação entre Contratante e contratada, bem como mecanismos de registro de ocorrências, acompanhamento de solicitações, abertura de chamados, tratamento de incidentes e documentação das intervenções realizadas.

7.16.2. Considerando a criticidade do ambiente, a contratada deverá disponibilizar canais de atendimento compatíveis com a necessidade de suporte contínuo, especialmente para incidentes que possam afetar energia, climatização, segurança, conectividade, *racks*, monitoramento ou demais subsistemas essenciais do *data center*.

7.16.3. O registro de ocorrências é requisito necessário para garantir rastreabilidade, fiscalização contratual, medição de níveis de serviço, análise de causa raiz, histórico de manutenção e gestão de riscos operacionais.

7.16.4. O detalhamento dos canais de atendimento, prazos, severidades, indicadores, relatórios e penalidades deverá constar no Termo de Referência e nos instrumentos de gestão contratual.

7.17. Requisitos de capacitação e transferência de conhecimento:

7.17.1. A contratação deverá prever capacitação da equipe técnica indicada pelo Contratante, com o objetivo de possibilitar a operação, acompanhamento, fiscalização, manutenção básica e acionamento adequado dos sistemas implantados.

7.17.2. A capacitação deverá abranger, no mínimo, os principais componentes da solução, incluindo Sala Segura, energia, UPS, geração, climatização, *chillers*, RDHx, *In-Row*, controle de acesso, monitoramento, cabeamento, segurança, procedimentos de operação, resposta a incidentes e rotinas básicas de manutenção.

7.17.3. A exigência de treinamento se justifica pela necessidade de autonomia mínima da equipe do 7º CTA, redução da dependência operacional da contratada, melhoria da fiscalização contratual e mitigação de riscos durante a operação do ambiente.

7.17.4. A capacitação deverá ser preferencialmente presencial, com atividades práticas no ambiente instalado, documentação de apoio em português e instrutores com experiência comprovada em soluções de *data center*.

7.17.5. Os critérios objetivos de carga horária, número mínimo de participantes, avaliação de satisfação, repetição do treinamento em caso de aproveitamento insuficiente e custos associados deverão ser detalhados no Termo de Referência.

7.18. Requisitos de compatibilidade, integração e responsabilidade única:

7.18.1. A solução deverá ser entregue como ambiente integrado, cabendo à contratada assegurar a compatibilidade entre todos os equipamentos, *softwares*, licenças, sistemas, materiais, acessórios e serviços necessários ao funcionamento do *data center*.

7.18.2. Ainda que sejam utilizados produtos de diferentes fabricantes ou que haja subcontratação parcial autorizada, a responsabilidade pela integração, interoperabilidade, desempenho, garantia, suporte, documentação, comissionamento e funcionamento global da solução deverá permanecer com a contratada.

7.18.3. Esse requisito é essencial porque a expansão do DC RF envolve subsistemas interdependentes, nos quais a falha de um componente pode comprometer a disponibilidade do conjunto. A responsabilidade única evita fragmentação de obrigações e reduz riscos de conflito entre fornecedores.

7.18.4. A contratada deverá garantir que todos os componentes necessários ao correto funcionamento da solução estejam incluídos na proposta, evitando fornecimentos incompletos, incompatibilidades futuras ou custos adicionais não previstos.

8. Estimativa da demanda - quantidade de bens e serviços

8.1. Para dimensionar as necessidades tecnológicas da expansão DC RF com intuito de hospedar servidores visando processamento de IA e atender as necessidades elencadas nos capítulos 4 e 5, considerando ainda que a solução precisa ser suficiente por pelo menos 10 (dez) anos e com capacidade de expansão, faz-se necessário observar:

8.1.1. A quantidade de *racks* que serão necessários para atender à demanda;

8.1.2. Infraestrutura elétrica do *data center* para suportar a potência energética a ser consumida;

8.1.3. O sistema de climatização para refrigerar os servidores estimados; e

8.1.4. As normas que o projeto deve atender.

8.2. Quantidade de *racks*:

8.2.1. O DC RF está sendo projetado para suportar uma carga de processamento de alta performance (SIIA), com um POD de IA com 12 (doze) *racks* de alta densidade de potência (65 kW/ *Rack*) mais dois POD de média densidade (15 kW/ *Rack*).

8.2.2. Cada *rack* de IA será dimensionado para suportar uma densidade energética nominal de 65 kVA, atendendo aos requisitos de *hardware* de última geração para IA, com GPUs NVIDIA (H200, B200 ou B300), podendo alcançar a ordem de 100 GPUs desse tipo ou mais (considerando o existente e o que está sendo solicitado em curto espaço de tempo, observa-se que o Exército Brasileiro atualmente já demanda de 50 GPUs).

8.2.3. A infraestrutura será montada inicialmente com refrigeração a ar otimizada e com espaços para garantir eventual instalação de tubulação para *Liquid Cooling* caso necessário no futuro.

8.2.4. Justificativa do Quantitativo e da Alta Densidade:

8.2.4.1. A escolha por instalar *racks* de 65 kVA fundamenta-se na inflexão tecnológica causada pelos *workloads* de IA.

8.2.4.2. Diferente de um *data center* corporativo convencional, onde *racks* operam entre 5 kVA e 10 kVA, o treinamento e processamento de modelos de IA, inclusive com grandes volumes de dados (como os demandados pelo supercomputador do CENSIPAM), exigem densidades que tornam a infraestrutura tradicional obsoleta.

8.2.4.3. A alta densidade busca ainda a Eficiência de Espaço e Custo, hospedando grande carga de TI em menos *racks* e reduzindo *footprint* da área crítica em até 40%, otimizando os custos de construção da sala segura.

8.2.4.4. A possibilidade de receber tecnologias de climatização distintas (*Air* ou *Liquid Colling*) é com o intuito de permitir, caso necessário, para que cada novo par de *racks* adicionado, implantação de soluções como D2C (*Direct-to-Chip*) ou RDHx com o mínimo de intervenção física, preservando a continuidade do serviço, conforme exigido pela certificação Tier III.

8.2.4.5. A possibilidade de expansão de mais 2 (dois) POD de *Racks* Padrão (densidade média de carga) se justifica pelo crescente aumento de demanda de infraestrutura e equipamentos dentro do *data center*, ao se observar os últimos anos. Como forma de se preparar para as demandas futuras, é importante ter infraestrutura preparada para suportar novas tecnologias e equipamentos.

8.3. Infraestrutura elétrica:

8.3.1. Novamente, diferente de ambientes de TI comuns, o processamento de IA exige suporte para Densidade Elétrica Extrema, variando de 30 kW a 100 kW por *rack*. Computando o POD de IA (**800 kW)** mais os outros dois POD Padrão de Servidores **(165 kW cada)**, teremos uma nova carga de TI adicionada de aproximadamente **1130 kW**. Para isso, as seguintes estruturas devem ser dimensionadas:

8.3.1.1. Cabines Elétricas, Transformadores e Distribuição.

8.3.1.2. Entrada de Energia: a atual subestação do CITEx possui potência Instalada de aproximadamente 6 MVA embora a potência máxima que pode ser demandada para a subestação do *Data Center* é atualmente de 1 MVA por linha, limitada pelo transformador. Desta forma, para se aumentar a capacidade de alimentação pela concessionária de energia para o *Data Center*, devem ser instalados mais 2 (dois) transformadores de 1,5 MVA cada, um para cada linha (2N).

8.3.1.3. Distribuição Interna: previsão de cabeamento elétrico com bitola adequada a fim de suportar a alta carga de TI, bem como de PDUs de alta capacidade em cada *rack* para evitar quedas e sobrecargas devido ao processamento massivo.

8.4. Sistema UPS:

8.4.1. Para sustentar a infraestrutura de IA e atender aos requisitos de Recertificação TIER III (*Uptime Institute*), o sistema de UPS deve garantir a manutenção simultânea, com uma configuração de UPS modulares e redundantes.

8.4.2. O chassi do **sistema UPS** será dimensionado para a carga final prevista do projeto, permitindo que novos módulos de potência (preferencialmente *hot-swappable*) sejam inseridos conforme o acréscimo de *racks*, sem a necessidade de substituição da base instalada.

8.4.3. Deve possuir Proteção de Cargas Sensíveis, preferencialmente com tecnologia "*True On-Line*" e com baterias de lítio para assegurar a integridade do *hardware* de alto custo (GPUs) contra flutuações da rede.

8.4.4. Dimensionamento:

8.4.4.1. Considerando a carga de TI do POD de IA, deverá ser instalado um Sistema UPS para suportar **800 kW** durante 5 min. Essa UPS deve ser específica para as flutuações de processamento de IA.

8.4.4.2. Adicionalmente, para se garantir o resfriamento do tipo *continuous cooling* deve ser instalado um outro UPS com capacidade de suportar as máquinas de clima, previstas em torno de **350 kW**, também para o tempo de 5 min.

8.4.4.3. Para a expansão dos dois novos POD Padrão, será necessário o acréscimo de 2 (dois) outros módulos UPS de **165 kW** suportando também 5 min. Esses dois POD não precisarão de UPS para clima pois não haverá necessidade de *continuous cooling.*

8.5. Grupo Motor Gerador (GMG) e Autonomia:

8.5.1. O sistema de geração secundária por meio de GMG deve redundante, a fim de atender a recertificação, e ser capaz de suportar a carga de TI e todo o ecossistema de climatização do *data center*.

8.5.2. O projeto considera os atuais geradores (2 geradores de 1 MVA cada) e respectiva capacidade de carga para compor a oferta elétrica necessária, otimizando o custo-benefício da contratação.

8.5.3. Com isso, deve-se prever adição modular de novos grupos geradores integrados ao barramento em consonância a cada incremento significativo da carga de pico.

8.5.4. Com a estratégia de crescimento modular, justifica-se a seguir a forma de aquisição dos novos geradores são:

8.5.4.1. Potência Nominal Sugerida do novo GMG é de 1 MVA por apresentar o melhor custo-benefício, maior oferta de manutenção com margem de segurança e considerando os padrões do mercado brasileiro.

8.5.4.2. A adoção de 2 (duas) unidades de 1 MVA facilita o balanceamento da nova usina de energia expandida, uma vez que o DC RF já opera com 2 (dois) geradores de 1 MVA (1000 kVA) cada, além de melhor aproveitar os espaços dos *slotes* reservados para expansão.

8.5.4.3. Com isso haverá a composição final de 4 (quatro) geradores de 1 MVA operando no regime 3 + 1, onde o quarto é redundância dos demais. Esses geradores estarão inseridos em uma mesma barra de paralelismo totalizando uma geração máxima de 3 MVA.

8.5.5. Dimensionamento Total e Redundância:

8.5.5.1. A estratégia de crescimento prevê atingir uma carga crítica de TI de 800 kW (para 12 *racks* de 65 kVA), que somada à carga de climatização (*chillers*, bombas e ventiladores), considerando ainda ambientes de IA de alta densidade, pode representar um acréscimo de 50% na demanda, obtendo uma carga total do *site* expandido em torno de 1.200 kW. Adicionalmente haverá a instalação de 2 (dois) outros POD de 165 kW de carga de TI.

8.5.5.2. Logo, para o estado final em intento, a contratação deve prever aquisição de 2 (dois) unidades de GMG de 1 MVA, com uma capacidade total de 3000 kVA.

8.5.5.3. Em um regime de redundância N+1 (considerando que 1 gerador poderia estar em manutenção ou falha, sobrando 3 ativos), o sistema entregaria 3000 kVA útil, cobrindo a carga máxima de 2.300 kVA com margem de segurança.

8.5.6. As tabelas a seguir demonstram a comparação de sistemas GMG conforme a redundância N+1 e 2N

5.5.6.1. Redundância N+1:

Marca	Quant.	Potência	Operação	Curso Unitário	Custo Total
Stemac	2	**1000 kVA**	N + 1	R$ 950.000,00	R$ 1.900.000,00

Volvo	2	**1000 kVA**	N + 1	R$ 1.050.000,00	R$ 2.100.000,00
Cummins	2	**1000 kVA**	N + 1	R$ 1.050.000,00	R$ 2.100.000,00
Caterpillar	2	**1000 kVA**	N + 1	R$ 1.250.000,00	R$ 2.500.000,00
Generac	2	**1000 kVA**	N + 1	R$ 1.200.000,00	R$ 2.4000.000,00

5.5.6.2. Redundância 2N:

Marca	Quant.	Potência	Operação	Curso Unitário	Custo Total
Stemac	2	**1500 kVA**	2N	R$ 125.000,00	R$ 2.500.000,00
Volvo	2	**1500 kVA**	2N	R$ 1.450.000,00	R$ 2.500.000,00
Cummins	2	**1500 kVA**	2N	R$ 1.500.000,00	R$ 3.000.000,00
Caterpillar	2	**1500 kVA**	2N	R$ 1.850.000,00	R$ 3.300.000,00
Generac	2	**1500 kVA**	2N	R$ 1.800.000,00	R$ 3.6000.000,00

8.5.7. Embora a opção por uma estrutura com redundância 2N seja mais robusta, do ponto de vista operacional, a opção por equipamentos de 1,5 MVA poderia aumentar o valor em até R$ 1.200.000,00, além do aumento de custos de logística e instalação. A opção por geradores maiores também limita a disponibilidade de peças para manutenção e mão de obra. Desta forma, é mais viável operacionalmente e economicamente geradores menores, sendo portanto demandados 2 (dois) geradores de 1 MVA.

8.6. Sistema de climatização:

8.6.1. A indústria de TI atingiu um ponto de inflexão onde servidores de IA de última geração (como plataformas NVIDIA) possuem processadores (GPUs) com (TDP) superior a 1.000W, exigindo soluções otimizadas de resfriamento.

8.6.2. Dada essa alta carga e a necessidade de recertificação TIER II, o sistema de *Chiller* apresenta melhor custo-benefício (ROI) e eficiência, dado que a carga de TI planejada já ultrapassa os 500 kW.

8.6.3. A estratégia para o sistema de climatização considera uma abordagem com vistas a duas tecnologias — Air Cooling e Liquid Cooling —, adotando inicialmente Air Cooling assistido por chillers indoor com condensadoras externas/remotas, e prevendo espaço na infraestrutura física para instalação futura, se necessário, de tubulações de aço inox, coletores, válvulas, engates rápidos e CDUs necessários ao sistema de climatização baseado em Liquid Cooling.

8.6.4. O sistema deve atender toda a carga de TI, mantendo a conformidade com a certificação Tier III, tendo unidades de ar-condicionado de precisão em ambiente confinado (corredor frio/quente) e os equipamentos *chillers* redundantes (N+1).

8.6.5. O sistema *Chiller* deve possuir tecnologia *Free Cooling* (usar o ar externo frio para resfriar o sistema sem ligar os compressores).

8.6.6. Não haverá central de água gelada e tanques de termoacumulação, cujo papel de *buffer* será desempenhado pelo *Nobreak*.

8.6.7. Justificativa Técnica e Eficiência Operacional:

8.6.7.1. A adoção de tecnologias avançadas (como *chillers* com *Free cooling*) para suportar alta densidade visa também otimizar o *Power Usage Effective* (PUE), garantindo que o custo de energia não inviabilize a operação. Para a solução proposta é esperado que o PUE seja inferior a 1,5.

8.6.7.2. A estratégia de uma abordagem com duas tecnologias – *Air Cooling* e *Liquid Cooling* – possui finalidade de permitir uma transição suave entre elas caso necessário, evitando gasto imediato com módulos de Unidades de Distribuição de Líquido Refrigerante (CDU) e com placas frias e eliminando o risco de futuras obras civis invasivas ou paradas de sistema quando a densidade exigir a migração para *Direct-to-Chip* (D2C).

8.6.8. Para o sistema de climatização In-Row destinado ao POD de Inteligência Artificial, a capacidade térmica mínima operacional requerida é de 300 kW. A capacidade total instalada poderá alcançar 360 kW, considerando a redundância necessária à operação em configuração N+1. Assim, os valores de 300 kW e 360 kW representam, respectivamente, a capacidade útil mínima exigida e a capacidade instalada total com redundância, não havendo divergência entre as especificações.

8.7. Consolidação dos quantitativos dos componentes da solução:

Item	Componente da solução	Quantidade	Classificação
1	Expansão de capacidade, Sala Segura, passagens seladas, piso, forro, quadros, PDUs, aterramento e certificação Uptime	1	Serviço
2	Sistema ininterrupto de energia - UPS para infraestrutura crítica de IA (UPS para climatização, baterias de lítio e infraestrutura associada)	1	Material
3	Sistema ininterrupto de energia - UPS para carga crítica de IA (UPS para POD padrão de servidores)	2	Material
4	Grupos moto geradores, chave de transferência automática, disjuntores de interligação e sistema de tanque para reabastecimento	2	Material
5	Sistema de climatização de alta densidade com chiller indoor e condensadora para atendimento ao sistema Rear Door	1	Material
6	Sistema de climatização com máquinas In-Row e condensadoras para atendimento ao POD de IA	1	Material
7	Sistema de climatização com máquinas In-Row e condensadoras para atendimento ao POD Padrão de Servidores	2	Material
8	Transformadores de Potência e interligação elétrica de média para baixa tensão	2	Material
9	Racks com Rear Door para alta densidade térmica	12	Material
10	Racks preparados para evolução futura com liquid cooling	6	Material
11	Conjunto de Racks Padrão para Servidores montados em POD	2	Material
12	Racks de rede e telecomunicações com interconexões	4	Material
13	Cabeamento estruturado entre racks de telecomunicações e racks de IA	1	Serviço
14	Cabeamento estruturado do Racks de Telecom para Racks do POD Padrão de Servidores	2	Serviço
15	Expansão do sistema de segurança, CFTV, videowall e controle de acesso	1	Serviço
16	Serviços de movimentação — moving — de ativos de TIC	25	Serviço

8.7.1. Os quantitativos consolidados na tabela anterior representam o dimensionamento máximo planejado da solução, necessário à definição da capacidade da infraestrutura, à estimativa de custos e à definição dos limites da contratação, não significando que todas as quantidades indicadas serão necessariamente demandadas pela Administração.

8.7.2. Ressalvadas as situações específicas descritas nos subitens seguintes, os quantitativos dos componentes da solução encontram-se tecnicamente definidos com base nas capacidades elétrica, térmica, física e operacional estabelecidas neste ETP.

8.7.3. Os quantitativos dos itens 9 e 10 representam possibilidades de composição do POD de IA, cuja capacidade total prevista é de 12 (doze) posições de racks de TI. A quantidade efetivamente contratada de

racks com Rear Door e de racks preparados para resfriamento a líquido será definida conforme a evolução tecnológica dos servidores de IA, a disponibilidade das soluções no mercado e as necessidades identificadas no momento da contratação.

8.7.3.1. Dessa forma, os quantitativos dos itens 9 e 10 não devem ser interpretados de forma cumulativa para composição de um único POD de IA, devendo a soma dos racks efetivamente contratados para esse POD observar o limite de 12 (doze) unidades. Exemplificativamente, poderão ser adotadas composições como 8 (oito) racks com solução baseada em air cooling/Rear Door e 4 (quatro) racks preparados para liquid cooling, ou outra distribuição tecnicamente adequada, respeitados os limites registrados para cada item.

8.7.3.2. A flexibilidade decorre da rápida evolução tecnológica dos equipamentos destinados ao processamento de Inteligência Artificial, especialmente quanto às exigências de dissipação térmica e aos modelos de refrigeração adotados pelos fabricantes de servidores, permitindo que a Administração ajuste a composição do POD às condições tecnológicas existentes quando da efetiva contratação.

8.7.4. O quantitativo de 4 (quatro) racks de Rede/Telecom previsto no item 12 decorre da arquitetura da solução, sendo destinados 2 (dois) racks de Telecom ao POD de IA e 1 (um) rack de Telecom para cada um dos 2 (dois) PODs padrão. Essa configuração foi dimensionada para suportar a quantidade prevista de conexões de cabeamento metálico UTP e óptico, bem como a concentração dos equipamentos de interconexão e distribuição necessários ao funcionamento dos respectivos PODs.

8.7.5. O quantitativo de 25 (vinte e cinco) unidades previsto para o serviço de movimentação — moving — corresponde aos ativos de TIC de maior criticidade cuja movimentação demandará execução especializada pela CONTRATADA, considerando os riscos relacionados ao desligamento, manuseio, transporte, reinstalação, reconexão e retorno à operação.

8.7.5.1. Os demais ativos que eventualmente necessitem ser movimentados durante a reorganização do ambiente serão tratados pela própria equipe técnica do 7º CTA, razão pela qual não integram o quantitativo contratado para o item 16.

9. Levantamento de soluções

9.1. Situação atual:

9.1.1. Inicialmente, será fornecida uma descrição da situação atual do DC RF em relação aos elementos relevantes para o estudo em questão. Além disso, serão destacados os aspectos comuns entre as possíveis soluções, seguidos pelas diferenças entre essas soluções.

9.1.2. No que diz respeito à alimentação de energia, o 7º CTA possui uma Cabine de Força Primária (CFP), localizada no CITEx (entrada lateral - frente a quadra residencial de oficiais). Nessa cabine, a energia é fornecida em média tensão (13,8 kV) e convertida pela Cabine de Transformação Elétrica (CTE) (item 5) para baixa tensão (220/380 VCA).

9.1.3. Para evitar indisponibilidade dos sistemas hospedados no 7º CTA, todas as soluções trabalham com segregação da rede elétrica desde a CFP. Ou seja, será criada uma infraestrutura elétrica para o DC RF totalmente segregada da alimentação elétrica do CITEx a partir da CFP. Assim, haverá uma CTE para o DC RF e outra para o CITEx (que permanecerá a atual CTE).

9.1.4. Para evitar custos de cabeamento de média tensão e aproveitar área já construída, a transformação de média tensão para baixa tensão será o mais próximo possível da CFP. Ou seja, a CTE do DC RF será próxima à CFP.

9.1.5. Para aproveitar a área construída e auxiliar na diminuição do ruído gerado pelo GMG que chega no pavilhão principal do CITEx/7º CTA, a sala do GMG foi construída já com dois slotes para instalação de dois novos geradores, visando a expansão, evitando assim a necessidade de geradores externos carenados.

9.1.8. A sala modular segura do DC RF deverá ter as seguintes dimensões: 15,5 (comprimento) x 8 ~ 9 (largura) x 3,2m (altura). Devido a posição das colunas, a largura variará de 8 m para 9 m a partir delas.

9.1.8. A seguir, são apresentadas 4 (quatro) soluções estudadas, das quais, 1 (uma) foi considerada mais viável tecnicamente, considerando os requisitos de espaço, capacidade, manutenção, energia, além de aspectos ligados a segurança da informação.

9.2. Levantamento das soluções:

9.2.1. Solução 1: Expansão da Sala Segura Modular dentro do DC RF:

9.2.1.1. A presente solução consiste na expansão da capacidade do *Data Center* Coronel Ricardo Franco (DC RF) por meio da implantação de uma Sala Segura em área técnica já existente no interior do próprio edifício do *data center*, localizada no pavimento térreo, conforme planejamento anteriormente concebido em 2014. Trata-se de espaço atualmente desocupado, já delimitado por estrutura em alvenaria, o que representa uma condição favorável para sua adaptação e aproveitamento, reduzindo a necessidade de ampliação externa da edificação e permitindo a expansão das capacidades computacionais dentro do próprio sítio.

9.2.1.2. Para viabilizar essa solução, será necessária a adequação integral do ambiente, de modo a transformá-lo em área apta a operar como sala segura para processamento crítico, contemplando a implantação de toda a infraestrutura necessária ao funcionamento de um *data center* que suporte carga de IA. Tal adequação deverá abranger, entre outros elementos, a estruturação da sala segura, sistemas elétricos, alimentação estabilizada, climatização de precisão, detecção e combate a incêndio, controle de acesso, monitoramento ambiental, cabeamento estruturado, infraestrutura de rede, preparação para instalação de *racks* e demais subsistemas indispensáveis à operação segura e contínua do ambiente. Os detalhamentos técnicos, quantitativos e requisitos específicos desta solução constarão do Termo de Referência e seus anexos.

9.2.1.3. Sob o ponto de vista institucional, esta alternativa apresenta como principal vantagem o fato de manter a expansão dentro da infraestrutura própria do Exército Brasileiro, preservando o controle físico, operacional e administrativo sobre o ambiente de processamento. Essa característica confere maior aderência às exigências de segurança da informação, soberania tecnológica, auditabilidade, cadeia de custódia dos ativos e proteção de dados sensíveis, especialmente relevantes em se tratando de cargas de trabalho estratégicas e de soluções voltadas ao processamento de inteligência artificial. Além disso, a utilização de área já existente no interior do próprio *data center* favorece a integração com a infraestrutura atualmente em operação, permitindo aproveitamento de parte do sítio técnico, da conectividade disponível, dos procedimentos internos de segurança e da governança já estabelecida para o DC RF.

9.2.1.4. Outro aspecto positivo desta solução é a sua adequação à necessidade de expansão estruturada e permanente da capacidade institucional, permitindo que o ambiente seja concebido desde a origem para suportar requisitos de maior criticidade, maior densidade computacional e futura evolução tecnológica. Diferentemente de soluções temporárias ou dependentes de terceiros, a expansão interna no próprio *data center* possibilita que o Exército defina integralmente os padrões construtivos, os níveis de redundância, os requisitos de resiliência, os controles de segurança física e lógica, bem como a arquitetura de energia, refrigeração e suporte necessária ao atendimento das demandas presentes e futuras do ambiente.

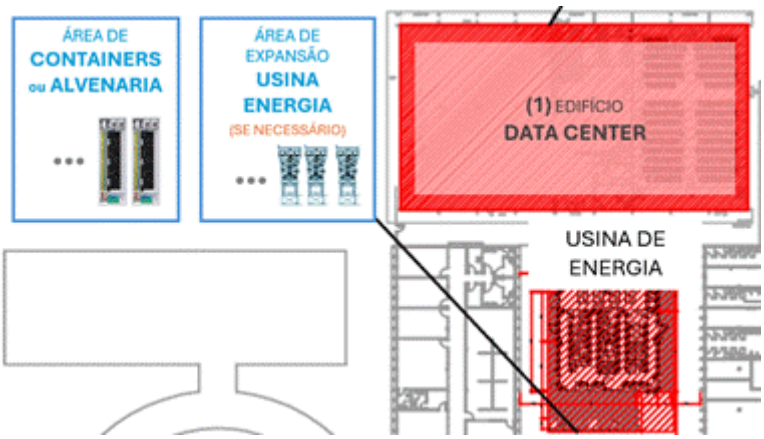
9.2.1.5. Todavia, trata-se de solução que demanda considerado investimento inicial, maior esforço de implantação e execução coordenada de serviços técnicos especializados de implantação e integração de infraestrutura de Data Center. Também requer avaliação minuciosa da compatibilidade da área com os requisitos estruturais, elétricos, térmicos e operacionais necessários ao novo ambiente, sobretudo quando se considera a possibilidade de instalação de equipamentos de maior densidade, como servidores acelerados por GPU, *storages* de alto desempenho e demais componentes associados ao processamento de IA. Além disso, por se tratar de intervenção no próprio sítio do DC RF, a execução deverá ser cuidadosamente planejada, a fim de mitigar impactos sobre a operação existente e preservar a continuidade dos serviços atualmente prestados.

9.2.1.6. Não obstante tais desafios, esta solução se mostra, em princípio, a mais aderente ao interesse estratégico da Administração, por combinar aproveitamento de área já disponível, fortalecimento da infraestrutura própria, maior controle institucional sobre ativos e informações críticas e melhor alinhamento com a necessidade de expansão segura e duradoura do *data center* do Exército. Assim, a implantação da Sala Segura Modular dentro do DC RF configura-se como alternativa tecnicamente consistente para ampliação da capacidade instalada, desde que acompanhada das adequações de infraestrutura necessárias e do correspondente planejamento executivo.

9.2.1.7. Foram realizadas 03 (três) cotações junto a empresas especializadas para esta solução, conforme registrado no documento de Memória de Cálculo. As propostas contemplam todos os bens e serviços previstos, tendo sido apurada média de custos no valor de R$ 63.400.000,00, a qual servirá de referência para análise comparativa de viabilidade econômica e subsidiará a estimativa preliminar da contratação.

9.2.2. Solução 2: Expansão modularizada do DC RF por *Container*:

9.2.2.1. A presente solução consiste na implantação de *data center* do tipo *container*, baseado no acoplamento de estruturas modulares padronizadas, projetadas especificamente para hospedar ambiente de processamento computacional crítico, com seus respectivos subsistemas de energia, climatização, monitoramento e segurança. Nessa alternativa, o(s) container(s) seria(m) instalado(s) em área externa adjacente ao piso térreo do Edifício Data Center e à área prevista para expansão da usina de energia, conforme indicado na figura abaixo. No que se refere à infraestrutura elétrica vinculada à usina de energia, esta solução adotaria, em essência, a mesma concepção prevista na Solução 1, especialmente quanto aos requisitos de alimentação, redundância e suporte ao novo ambiente.



9.2.2.2. Sob o ponto de vista técnico, essa alternativa apresenta como principal característica a utilização de estrutura pré-fabricada e especializada, concebida para rápida implantação e integração com os sistemas necessários ao funcionamento de um *data center*. Em comparação com soluções que demandam adaptação integral de ambiente construído, o modelo em *container* tende a reduzir a dependência de intervenções mais extensas de engenharia civil, uma vez que parte significativa da infraestrutura já é concebida de forma integrada pelo fabricante. Dessa forma, a solução se mostra potencialmente vantajosa em cenários nos quais se busca celeridade de implantação, padronização construtiva e expansão da capacidade computacional em prazo inferior ao exigido por soluções convencionais.

9.2.2.3. Entre as principais vantagens desta alternativa, destaca-se, inicialmente, o menor tempo de implantação, tendo em vista que os módulos podem ser fabricados, preparados e parcialmente integrados previamente, reduzindo o tempo de execução no local. Soma-se a isso a menor dependência de obras civis complexas, o que pode simplificar etapas da implantação e reduzir parte dos riscos inerentes a intervenções em estruturas já existentes. Outro benefício relevante é a modularidade, que permite expansão incremental da capacidade, conforme a evolução da demanda institucional. Além disso, trata-se de solução com potencial de realocação futura, caso haja necessidade estratégica de transferência da estrutura para outro local, conferindo maior flexibilidade ao investimento realizado.

9.2.2.4. Entretanto, a solução em *container* também apresenta desvantagens e limitações relevantes, que devem ser consideradas no estudo técnico. Embora reduza parte das intervenções civis, ela continua exigindo infraestrutura de suporte no local de instalação, especialmente fundações adequadas, interligações elétricas, sistemas de conectividade, drenagem, aterramento, proteção contra descargas atmosféricas, segurança física perimetral e eventual integração com sistemas de combate a incêndio e monitoramento. Além disso, por se tratar de estrutura instalada em área externa, o ambiente pode ficar mais exposto a fatores ambientais, exigindo cuidados adicionais quanto à proteção física, controle de acesso, durabilidade e manutenção.

9.2.2.5. Outro aspecto relevante diz respeito à integração operacional e à aderência ao contexto de missão crítica. Embora o *data center* em *container* possa atender a demandas de processamento e armazenamento, sua adequação para cargas mais sensíveis ou de alta criticidade, especialmente aquelas voltadas a aplicações estratégicas e ao processamento de inteligência artificial, deve ser avaliada com rigor. Isso porque cargas de IA podem demandar maior densidade elétrica, maior capacidade térmica, refrigeração mais robusta e condições estruturais específicas para operação contínua e segura. Nesses casos, é necessário verificar se a solução ofertada suporta, de forma comprovada, os requisitos de potência, climatização, peso por *rack*, disponibilidade e resiliência exigidos pelo ambiente pretendido.

9.2.2.6. Do ponto de vista institucional, também se observa que, embora o *container* permaneça sob domínio do Exército Brasileiro e dentro de área controlada, trata-se de uma solução que pode ser percebida como menos integrada e menos permanente do que a expansão de ambiente seguro no interior do próprio edifício do *data center*. Dessa forma, sua adoção pode ser mais adequada em cenários de expansão acelerada, necessidade transitória, reforço complementar de capacidade ou implantação em fases, do que como solução definitiva para todo o núcleo principal de processamento estratégico.

9.2.2.7. Em síntese, a solução de *data center* em container apresenta-se como alternativa tecnicamente viável para expansão modular, rápida e com menor dependência de obras civis, destacando-se pela flexibilidade de implantação e pela possibilidade de futura realocação. Por outro lado, requer análise criteriosa quanto à sua integração com a infraestrutura existente, à segurança física do ambiente externo, à robustez necessária para cargas críticas e à sua real aderência às demandas de longo prazo do Exército Brasileiro, especialmente no contexto de processamento intensivo e estratégico de IA.

9.2.2.8. Para esta solução, foi obtido 01 (um) orçamento junto a empresa especializada, conforme registrado no documento de Memória de Cálculo, no valor de R$ 66.650.000,00. Tal valor servirá como referência preliminar para fins comparativos no estudo, ressalvando-se que, por se tratar de quantitativo ainda limitado de cotações, a estimativa poderá demandar complementação em etapas posteriores de aprofundamento técnico e de consolidação da pesquisa de mercado.

9.2.3. Solução 3: *Colocation* de equipamentos:

9.2.3.1. A solução de ***colocation*** consiste na instalação dos equipamentos computacionais, de armazenamento e de rede do Exército Brasileiro em infraestrutura de *data center* pertencente a terceiro especializado, sendo Empresa Privada ou Órgão Público, o qual passa a prover o espaço físico, a alimentação elétrica, a climatização, a proteção contra incêndio, a conectividade e os controles de

segurança física do ambiente. Nesse modelo, os ativos de tecnologia permanecem sob propriedade e gestão da Administração, enquanto a infraestrutura predial e os serviços associados ao ambiente de hospedagem são disponibilizados pela contratada.

9.2.3.2. Sob a perspectiva técnica, a adoção de *colocation* apresenta como principais vantagens a celeridade de implantação, a redução da necessidade de investimentos imediatos em obras civis e infraestrutura crítica, bem como a possibilidade de ampliação relativamente rápida da capacidade instalada, sem que seja necessário aguardar a conclusão de expansão física no *data center* próprio. Trata-se, portanto, de alternativa potencialmente útil em cenários que demandem rápida disponibilização de capacidade computacional, inclusive para absorção de crescimento temporário, implantação de ambientes de contingência, continuidade de serviços ou atendimento emergencial de novas demandas.

9.2.3.3. Todavia, para o contexto do Exército Brasileiro, especialmente quando se considera a hospedagem de dados sensíveis, informações críticas e cargas computacionais estratégicas, inclusive aquelas relacionadas a processamento de inteligência artificial, a solução de *colocation* impõe limitações relevantes. Embora o ambiente contratado possa dispor de controles de segurança física e lógica compatíveis com padrões de mercado, permanece o fato de que os ativos institucionais ficariam instalados em infraestrutura externa, operada por terceiro, o que amplia riscos associados à dependência contratual, à exposição indireta da arquitetura tecnológica, à circulação de pessoal externo em ambiente sensível, à necessidade de intervenções técnicas compartilhadas e à redução do nível de controle soberano sobre a instalação física.

9.2.3.4. Além disso, no caso específico de um *data center* voltado ao processamento de IA, a solução de *colocation* exige avaliação ainda mais rigorosa, uma vez que cargas dessa natureza podem demandar elevada densidade elétrica por *rack*, sistemas avançados de climatização e, em determinados cenários, soluções especializadas de refrigeração. Assim, não basta a existência genérica de um serviço de *colocation*, é indispensável verificar se a infraestrutura ofertada comporta, de forma comprovada, os requisitos de potência, peso, refrigeração, conectividade, segregação física e disponibilidade exigidos para o ambiente pretendido.

9.2.3.5. Outro aspecto a ser considerado é a eventual restrição de oferta local, sobretudo quando se busca solução com alto nível de disponibilidade, suporte a cargas de alta densidade e requisitos robustos de segurança. Em Brasília, diferentemente de São Paulo, ainda não existe oferta de *data center* com capacidade para suportar equipamentos de IA, o que restringe essa solução. Na prática, a concretização desse Projeto pode inserir o DC Cel Ricardo Franco, como o primeiro *data center* de IA do Centro Oeste.

9.2.3.6. Dessa forma, a solução de *colocation* pode ser considerada viável como alternativa complementar, transitória, contingencial ou destinada a cargas menos sensíveis, especialmente quando houver necessidade de rápida expansão de capacidade. Entretanto, para o núcleo principal de processamento estratégico do Exército, notadamente aquele voltado a dados críticos e aplicações de inteligência artificial de maior relevância institucional, sua adoção demanda análise restritiva e condicionada à comprovação de requisitos elevados de segurança, segregação, desempenho e governança. Assim, em princípio, o *colocation* não se apresenta como a solução mais adequada para substituição integral da infraestrutura própria, podendo, contudo, compor estratégia híbrida de expansão, desde que devidamente limitado e controlado.

9.2.4. Solução 4: Hospedagem em nuvem:

9.2.4.1. A solução de hospedagem em nuvem consiste na utilização de recursos computacionais disponibilizados sob demanda por provedor externo, com provisionamento elástico e acesso via rede, podendo abranger, conforme o modelo contratado, capacidades de Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e *Software* como Serviço (SaaS). No âmbito do SISP, sua contratação deve observar o processo previsto na Instrução Normativa SGD/ME nº 94/2022 e o modelo instituído pela Portaria SGD/MGI nº 5.950/2023, de uso obrigatório nos processos iniciados a partir de 30 de abril de 2024.

9.2.4.2. Sob a ótica estritamente técnica e operacional, a hospedagem em nuvem apresenta vantagens conhecidas, como elasticidade, rápido provisionamento, expansão sob demanda, potencial otimização do

uso de recursos e redução da necessidade de investimentos imediatos em infraestrutura física própria. Tais atributos tornam essa alternativa atrativa para cenários de crescimento variável, ambientes de desenvolvimento, testes, cargas não críticas e serviços cuja continuidade possa ser suportada por arquitetura fortemente dependente do provedor.

9.2.4.3. Entretanto, para o contexto deste estudo, que trata da sustentação de Soluções de Infraestrutura de IA e do processamento de cargas de trabalho estratégicas do Exército Brasileiro, a alternativa de hospedagem em nuvem de terceiros, especialmente em nuvem pública ou híbrida, não se mostra a mais adequada como solução principal. A regulamentação federal atualmente exige classificação prévia da informação e estabelece que a escolha do modelo de nuvem deve considerar o nível de sigilo da carga de trabalho. O modelo oficial do Governo Digital determina que informações e cargas de trabalho com restrição legal de acesso devem, como regra, permanecer em Nuvem de Governo, e veda o tratamento, em nuvem pública, de informações classificadas em grau de sigilo e de documentos preparatórios que possam originá-las.

9.2.4.4. Além disso, a disciplina específica publicada pelo Gabinete de Segurança Institucional, em outubro de 2025, passou a admitir o tratamento, em nuvem, de informações classificadas nos graus reservado e secreto apenas em nuvem privada ou comunitária, com *data centers* localizados exclusivamente em território nacional, infraestrutura dedicada, provedor habilitado e auditado, vedação de replicação ou *backup* fora do país e impedimento de acesso do provedor ao conteúdo das informações. A mesma norma mantém a proibição do uso de nuvem para informações ultrassecretas e informa expressamente que nuvem pública e híbrida permanecem vedadas para esse tipo de tratamento.

9.2.4.5. No caso específico de um ambiente de IA, os riscos tornam-se ainda mais sensíveis. A depender da arquitetura contratada, do modelo de serviço e das condições operacionais do provedor, pode haver ampliação da exposição de dados, metadados, *logs*, artefatos de processamento, parâmetros de uso e rotinas operacionais críticas, o que é incompatível com a necessidade de controle soberano, cadeia de custódia, auditabilidade reforçada e continuidade operacional autônoma exigidas em contexto de Defesa. Soma-se a isso a dependência tecnológica e contratual de infraestrutura externa para cargas estratégicas, o que pode afetar a governança, a previsibilidade de custos, a portabilidade e a capacidade institucional de resposta em cenários de crise ou restrição operacional. Essa preocupação com maior controle estatal sobre dados sensíveis também aparece na própria implementação da Nuvem de Governo, descrita pelo MGI como infraestrutura sob responsabilidade direta da administração pública federal para proteção de dados sensíveis do Estado.

9.2.4.6. Dessa forma, conclui-se que a hospedagem em nuvem de terceiros não deve ser adotada, neste caso, como solução principal para o processamento estratégico da infraestrutura de IA do Exército Brasileiro. Sua utilização poderá ser eventualmente considerada apenas de forma restrita e complementar, em hipóteses específicas, tais como cargas sem restrição de acesso, ambientes temporários de desenvolvimento, testes controlados, processamento de dados públicos ou não sensíveis e serviços acessórios, sempre condicionada à classificação prévia da informação, ao mapeamento formal de riscos, à estratégia institucional de uso de nuvem e à aprovação da governança competente. Ressalva-se, ainda, que a Nuvem de Governo constitui arranjo distinto da nuvem pública de mercado, voltado justamente ao tratamento mais seguro de dados sensíveis sob governança estatal direta.

10. Análise comparativa de soluções

10.1. Premissas da análise comparativa:

10.1.1. A análise comparativa das soluções foi realizada com base nas necessidades de negócio, nas necessidades tecnológicas, nos requisitos técnicos e nas alternativas identificadas no levantamento de mercado, considerando a finalidade central da contratação: ampliar a capacidade operacional do *Data Center* Coronel Ricardo Franco (DC RF), de modo a permitir a hospedagem de infraestrutura de alta densidade destinada ao processamento de Inteligência Artificial (IA), com preservação da segurança, disponibilidade, soberania dos dados, continuidade operacional e aderência à certificação Tier III.

10.1.2. A necessidade administrativa não se limita à simples disponibilização de espaço físico ou capacidade computacional genérica. Trata-se da implantação de ambiente crítico, próprio, controlado e evolutivo, apto a suportar cargas de IA com elevada densidade elétrica e térmica, estimadas em até 65 kVA por *rack*, com arquitetura final de referência composta por 12 *racks* de alta densidade, carga crítica de TI de aproximadamente 780 kVA e planejamento de capacidade de até 800 kVA.

10.1.3. Dessa forma, a solução a ser escolhida deve atender simultaneamente aos seguintes objetivos: prover capacidade permanente de hospedagem para Soluções de Infraestrutura de IA; preservar o controle físico, operacional e administrativo pelo Exército Brasileiro; assegurar integração com a infraestrutura existente do DC RF; permitir evolução tecnológica da climatização, inclusive com preparação para eventual *liquid cooling*; manter a aderência à certificação Tier III; mitigar riscos de segurança da informação; e apresentar vantajosidade técnica e econômica ao longo do ciclo de vida da solução.

10.1.4. Foram analisadas quatro alternativas principais:

10.1.4.1. **Solução 1 - Expansão da sala segura modular dentro do DC RF**;

10.1.4.2. **Solução 2 - Expansão modularizada do DC RF por *container***;

10.1.4.3. **Solução 3 - *Colocation* de equipamentos**; e

10.1.4.4. **Solução 4 - Hospedagem em nuvem**.

10.2. Critérios utilizados na comparação:

10.2.1. Para fins de comparação, foram adotados critérios técnicos, operacionais, institucionais, econômicos e estratégicos, compatíveis com a natureza crítica da contratação. Os critérios avaliados foram os seguintes:

10.2.1.1. **Aderência à necessidade institucional**, considerando a capacidade de atendimento ao processamento estratégico de IA no âmbito do Exército Brasileiro;

10.2.1.2. **Soberania, segurança da informação e controle institucional**, considerando o grau de controle físico, lógico, operacional e administrativo sobre os ativos, dados, modelos, artefatos de IA, *logs*, metadados e rotinas críticas;

10.2.1.3. **Capacidade de suportar alta densidade elétrica e térmica**, especialmente *racks* de até 65 kVA, servidores acelerados por GPU, *storages* de alto desempenho e redes de alta velocidade;

10.2.1.4. **Integração com a infraestrutura existente do DC RF**, incluindo energia, climatização, monitoramento, segurança física, rede passiva, operação, governança e procedimentos internos;

10.2.1.5. **Preservação da disponibilidade e da certificação Tier III**, com manutenção da manutenibilidade concorrente e da continuidade operacional;

10.2.1.6. **Escalabilidade e evolução tecnológica**, considerando a possibilidade de expansão futura e transição entre tecnologias de resfriamento, especialmente de *air cooling* para *liquid cooling*;

10.2.1.7. **Riscos de implantação e operação**, incluindo riscos de segurança física, dependência de terceiros, interfaces externas, migração, indisponibilidade e complexidade de manutenção;

10.2.1.8. **Vantajosidade econômica**, considerando o custo preliminar levantado, os ustos adicionais, o aproveitamento de infraestrutura existente e o potencial custo total de propriedade;

10.2.1.9. **Permanência da capacidade institucional**, considerando se a solução gera ativo estratégico duradouro para o Exército ou apenas dependência contratual temporária; e

10.2.1.10. **Adequação ao ciclo de vida da solução**, incluindo operação, manutenção, suporte, capacitação, documentação, sustentabilidade e possibilidade de expansão ao longo dos anos.

10.3. Matriz comparativa sintética das soluções:

Critério de comparação	Solução 1 - Sala segura modular interna	Solução 2 - *Container*	Solução 3 - *Colocation*	Solução 4 - Nuvem
Aderência ao objetivo principal	Alta	Média	Baixa/Média	Baixa
Controle físico e operacional	Alto	Alto, porém com maior exposição externa	Reduzido, por depender de infraestrutura de terceiro	Reduzido, por depender de provedor externo
Soberania e proteção de dados	Alta	Alta, mas com maior superfície física de risco	Média/Baixa	Baixa para cargas estratégicas sensíveis
Integração com o DC RF	Alta	Média	Baixa	Baixa
Capacidade para alta densidade de IA	Alta, desde que projetada para esse fim	Possível, mas limitada pela geometria e configuração do módulo	Incerta e dependente da oferta do provedor	Variável, dependente do provedor e das restrições normativas
Preservação da certificação Tier III	Mais aderente, por integração ao sítio existente	Exige maior análise de interfaces externas	Depende da certificação do terceiro, sem controle integral do EB	Não substitui a certificação do ambiente próprio
Escalabilidade e evolução tecnológica	Alta	Média	Média, dependente de contrato e disponibilidade	Alta em elasticidade, mas limitada por segurança e governança
Preparação para *liquid cooling*	Alta, se prevista em projeto	Possível, porém mais condicionada ao módulo	Incerta	Dependente do provedor
Segurança física	Alta	Média, por instalação externa	Média, por depender de terceiro	Não aplicável ao ambiente físico próprio
Rapidez de implantação	Média	Alta	Alta	Alta
Geração de capacidade institucional permanente	Alta	Média	Baixa	Baixa
Dependência de terceiros	Baixa/Média	Média	Alta	Alta
Vantajosidade econômica preliminar	Melhor estimativa disponível: R$ 63.400.000,00	Estimativa superior: R$ 66.650.000,00	Estimativa recorrente R$ 20.100.000,00 e R$ 80.200.000,00 em 10 anos	Estimativa mínima R$ 71.600.000,00 em 10 anos.
Conclusão comparativa	**Mais aderente e recomendada**	**Viável tecnicamente, mas não como solução principal**	**Possível apenas de forma complementar ou contingencial**	**Não recomendada como solução principal**

10.4. Análise comparativa da Solução 1 - Expansão da Sala Segura Modular dentro do DC RF:

10.4.1. A Solução 1 consiste na implantação de Sala Segura Modular em área técnica já existente no interior do *Data Center* Coronel Ricardo Franco, localizada no pavimento térreo e anteriormente prevista para expansão da capacidade do ambiente. Essa alternativa permite aproveitar área já disponível, reduzir a necessidade de nova edificação externa e manter a ampliação dentro do próprio sítio técnico controlado pelo Exército Brasileiro.

10.4.2. Sob a ótica institucional, trata-se da solução de maior aderência à finalidade da contratação, pois preserva o controle físico, operacional e administrativo do ambiente de processamento pelo Exército, reduzindo

riscos associados à exposição de dados, ativos, modelos, artefatos de IA, *logs* e informações sensíveis em ambiente de terceiros.

10.4.3. A expansão interna também favorece a integração com a infraestrutura já existente do DC RF, incluindo conectividade, procedimentos de segurança, governança operacional, monitoramento, controle de acesso, rotinas de manutenção, sistemas de energia, climatização e proteção contra incêndio. Essa integração é relevante para preservar a continuidade dos serviços atualmente prestados e permitir que a nova capacidade de IA seja incorporada ao ambiente corporativo de forma controlada.

10.4.4. Do ponto de vista técnico, a Solução 1 permite que a Sala Segura seja concebida desde o projeto executivo para suportar os requisitos de alta densidade previstos no estudo, incluindo *racks* de até 65 kVA, carga crítica de até 800 kVA para o POD de IA, climatização de precisão, confinamento térmico, tecnologias de *rear door heat exchanger*, *in-row cooling*, preparação para *liquid cooling*, rede passiva de alta capacidade, monitoramento integrado e infraestrutura elétrica redundante. Além disso, a solução contempla a implantação de 2 PODs padrão adicionais, destinados à hospedagem de cargas convencionais de TIC, ampliando a capacidade geral do *data center* e permitindo melhor aproveitamento da infraestrutura instalada.

10.4.5. A Solução 1 também apresenta maior potencial de preservação da certificação Tier III, uma vez que a expansão pode ser concebida de forma integrada à topologia existente, observando os requisitos de manutenibilidade concorrente, redundância, continuidade operacional e compatibilidade entre projeto, implantação e operação.

10.4.6. Embora demande maior esforço de engenharia, coordenação de obras, planejamento executivo detalhado e investimento inicial relevante, essa solução gera capacidade institucional permanente, fortalece o *data center* próprio do Exército e reduz a dependência de provedores externos para o processamento estratégico de IA.

10.4.7. No aspecto econômico, a Solução 1 possui valor de referência atualizado de **R$ 63.400.000,00**, contemplando não apenas a infraestrutura do POD de IA, mas também a implantação de **2 (dois) PODs padrão** , incluindo estrutura, climatização, *nobreaks*/UPS adicionais, *racks*, adequações elétricas, cabeamento e demais componentes associados. Esse valor decorre de composição de preços por macrocomponentes da solução, com base em estimativa técnica de mercado, e reflete o escopo ampliado da contratação.

10.4.8. Dessa forma, a Solução 1 apresenta a melhor combinação entre aderência técnica, segurança institucional, controle soberano, integração ao ambiente existente, capacidade de evolução tecnológica, preservação da disponibilidade, formação de capacidade permanente e vantajosidade econômica preliminar.

10.5. Análise comparativa da Solução 2 - Expansão modularizada por *container*:

10.5.1. A Solução 2, baseada na implantação de *data center* modular em *container*, apresenta vantagens pontuais, especialmente quanto à velocidade de implantação, padronização construtiva, modularidade e possibilidade de realocação futura. Essas características podem torná-la útil em cenários emergenciais, transitórios, contingenciais ou de reforço temporário de capacidade.

10.5.2. Contudo, para a finalidade principal deste ETP, a solução por *container* apresenta menor aderência ao caráter permanente e estratégico da expansão pretendida. Embora permaneça em área sob domínio do Exército, o *container* seria instalado em área externa ao edifício principal do DC RF, o que amplia a superfície de exposição física e exige controles adicionais de segurança perimetral, drenagem, fundações, aterramento, SPDA, interligações elétricas, conectividade, monitoramento e combate a incêndio.

10.5.3. Além disso, a solução por container tende a ser menos flexível do ponto de vista arquitetônico, pois fica condicionada à geometria, aos limites estruturais, à capacidade térmica e ao arranjo proprietário do módulo adquirido. Isso pode reduzir a liberdade de evolução futura para novas tecnologias de resfriamento, expansão de *racks*, adequações de rede, rearranjos internos e implantação progressiva de infraestrutura *liquid cooling ready*.

10.5.4. No aspecto econômico, a Solução 2 deve ser comparada com o mesmo escopo da Solução 1, isto é, contemplando o POD de IA e os 2 PODs padrão. Considerando que a estimativa preliminar da solução por container era aproximadamente 5,11% superior à estimativa preliminar da expansão interna, a atualização

proporcional para o novo escopo indica valor comparativo mínimo de aproximadamente **R$ 66.650.000,00**. Esse valor deve ser interpretado como referência conservadora, pois a solução por container ainda tende a exigir custos adicionais de implantação externa, fundações, interligações elétricas e lógicas, segurança perimetral, proteção contra intempéries, integração com sistemas de incêndio, monitoramento e manutenção.

10.5.5. Assim, embora tecnicamente viável para cenários específicos, a Solução 2 não se mostra mais vantajosa do que a expansão interna da Sala Segura Modular, especialmente quando considerados permanência da capacidade, integração ao DC RF, segurança física, flexibilidade arquitetônica e economicidade preliminar.

10.6. Análise comparativa da Solução 3 - *Colocation* de equipamentos:

10.6.1. A Solução 3 consiste na instalação de equipamentos do Exército em *data center* de terceiro, público ou privado, com fornecimento de espaço físico, energia, climatização, segurança, conectividade e serviços associados pelo provedor de *colocation*.

10.6.2. A principal vantagem dessa alternativa é a possibilidade de disponibilização mais rápida de capacidade de hospedagem, com menor necessidade de obras civis imediatas e possibilidade de uso em cenários de contingência, recuperação de desastre, expansão temporária ou atendimento emergencial.

10.6.3. Todavia, para o núcleo estratégico de processamento de IA do Exército Brasileiro, o *colocation* apresenta limitações relevantes. A instalação dos ativos em infraestrutura externa reduz o controle físico e operacional direto da Administração, amplia a dependência contratual, aumenta a circulação de pessoal externo em ambiente sensível e pode expor, ainda que indiretamente, informações sobre arquitetura, topologia, densidade, consumo, redundância, conectividade e padrões operacionais.

10.6.4. No caso específico de IA de alta densidade, a adoção de colocation exigiria comprovação rigorosa de capacidade do provedor para suportar potência elevada por *rack*, peso, refrigeração, segregação física, conectividade, disponibilidade, baixa latência, segurança e evolução tecnológica. Essa comprovação não pode ser presumida, pois ambientes de IA e HPC possuem requisitos superiores aos de *data centers* corporativos convencionais.

10.6.5. Ademais, a solução de colocation não gera capacidade institucional permanente no DC RF. Ao final do contrato, permaneceriam riscos de renovação, migração física dos equipamentos, renegociação de custos, dependência de provedor, interconexões, suporte remoto, transporte, seguro e eventuais adequações impostas pelo ambiente de terceiro.

10.6.6. Dessa forma, o *colocation* pode ser considerado alternativa complementar, transitória ou contingencial, especialmente para cargas menos sensíveis ou situações emergenciais, mas não se apresenta como solução mais adequada para substituir a implantação de capacidade própria, segura e permanente de IA no *Data Center* Coronel Ricardo Franco.

10.7. Análise comparativa da Solução 4 - Hospedagem em nuvem:

10.7.1. A Solução 4 consiste na utilização de recursos computacionais sob demanda fornecidos por provedor externo de nuvem, abrangendo, conforme o modelo contratado, IaaS, PaaS ou SaaS.

10.7.2. Essa alternativa possui vantagens conhecidas, tais como elasticidade, rápido provisionamento, expansão sob demanda, redução de investimento inicial em infraestrutura física e disponibilidade de serviços gerenciados. Tais características podem ser úteis para desenvolvimento, testes, cargas públicas, ambientes temporários, serviços acessórios ou processamento de dados sem restrição de acesso.

10.7.3. Entretanto, a hospedagem em nuvem não atende adequadamente ao objetivo principal da presente contratação, que é estruturar capacidade própria, física, controlada e soberana para processamento estratégico de IA no âmbito do Exército Brasileiro.

10.7.4. Em ambientes de IA, os riscos de exposição não se limitam aos dados brutos, abrangendo também *prompts*, bases de treinamento, *embeddings*, vetores, *logs*, metadados, artefatos intermediários, parâmetros de execução, modelos ajustados, pesos e rotinas operacionais. A depender da arquitetura contratada e das

condições do provedor, tais elementos podem ampliar riscos de segurança, governança, rastreabilidade, cadeia de custódia e dependência tecnológica.

10.7.5. Além disso, o uso de nuvem para cargas estratégicas deve ser condicionado à classificação prévia da informação, à análise de riscos, às restrições normativas aplicáveis, à governança competente e à verificação da compatibilidade entre o modelo de serviço e o grau de sigilo dos dados processados. Para cargas críticas de Defesa, a nuvem pública ou híbrida não se mostra adequada como solução principal.

10.7.6. Portanto, a nuvem pode ser admitida apenas como recurso complementar, restrito e condicionado, voltado a cargas não sensíveis, testes controlados, processamento de dados públicos, desenvolvimento temporário ou serviços acessórios, não substituindo a necessidade de implantação de infraestrutura própria de IA no DC RF.

10.8. Comparação quanto à segurança, soberania e controle institucional:

10.8.1. Sob o critério de segurança, soberania e controle institucional, a Solução 1 apresenta a maior aderência, pois mantém a infraestrutura dentro do próprio *Data Center* do Exército, sob controle direto da Administração, com menor exposição física e lógica, maior rastreabilidade, maior governança sobre ativos e maior capacidade de aplicar controles internos de segurança.

10.8.2. A Solução 2 também preserva a propriedade e o controle institucional, mas aumenta a superfície de exposição por estar localizada em ambiente externo ao edifício principal, exigindo camadas adicionais de segurança perimetral, controle de acesso, monitoramento, proteção contra intempéries e resposta a incidentes.

10.8.3. A Solução 3 reduz o controle direto da Administração, pois transfere a sustentação física do ambiente para terceiro, ainda que os equipamentos permaneçam sob propriedade do Exército.

10.8.4. A Solução 4 apresenta o menor grau de controle físico e operacional, pois depende de infraestrutura externa, modelo contratual do provedor e regras específicas de governança, sendo inadequada como solução principal para dados e cargas estratégicas de Defesa.

10.8.5. Conclui-se, portanto, que a Solução 1 é a mais aderente ao requisito de soberania e controle institucional.

10.9. Comparação quanto à capacidade técnica para IA de alta densidade:

10.9.1. A Solução 1 permite projetar a infraestrutura desde a origem para cargas de IA de alta densidade, incluindo energia crítica, climatização especializada, *rear door heat exchangers*, *in-row cooling*, confinamento térmico, *racks* de alta capacidade estrutural, rede passiva de alta performance, sensores, monitoramento e preparação para *liquid cooling*.

10.9.2. A Solução 2 pode ser concebida para alta densidade, mas apresenta limitações decorrentes da configuração modular do *container*, da geometria interna, dos limites de expansão, das interfaces externas e da dependência de soluções proprietárias.

10.9.3. A Solução 3 depende integralmente da capacidade do provedor de *colocation*, sendo indispensável comprovação de suporte a densidade elétrica, térmica, estrutural e lógica compatível com IA. Como essa capacidade não é inerente a qualquer *data center* de mercado, há incerteza técnica relevante.

10.9.4. A Solução 4 pode ofertar recursos computacionais de IA sob demanda, mas não resolve o problema de implantação de infraestrutura própria, física, controlada e preparada para cargas estratégicas, além de estar sujeita a restrições normativas e riscos de governança.

10.9.5. Assim, quanto à capacidade técnica para IA de alta densidade, a Solução 1 apresenta maior previsibilidade, maior controle de projeto e maior aderência à necessidade final.

10.10. Comparação quanto à disponibilidade, continuidade operacional e Tier III:

10.10.1. A Solução 1 é a que melhor permite preservar a aderência à certificação Tier III do DC RF, pois a expansão pode ser projetada, implantada, comissionada e recertificada em compatibilidade com a topologia existente, observando redundância, manutenibilidade concorrente e continuidade operacional.

10.10.2. A Solução 2 exigiria análise mais complexa de interfaces entre o container e a infraestrutura do DC RF, especialmente quanto a energia, climatização, conectividade, segurança, incêndio, monitoramento e manutenção concorrente.

10.10.3. A Solução 3 dependeria da certificação, dos procedimentos e da governança do provedor de *colocation* , sem assegurar o mesmo grau de controle institucional sobre a manutenção concorrente e sobre a evolução da infraestrutura.

10.10.4. A Solução 4 não preserva nem amplia diretamente a certificação Tier III do ambiente próprio do Exército, pois desloca a capacidade computacional para ambiente externo e não substitui a necessidade de infraestrutura física própria para cargas críticas.

10.10.5. Dessa forma, a Solução 1 é a alternativa mais compatível com a preservação da disponibilidade e da certificação Tier III do *Data Center* Coronel Ricardo Franco.

10.11. Comparação quanto à economicidade e custo-benefício:

10.11.1. A Solução 1 apresenta valor de referência atualizado de **R$ 63.400.000,00**, contemplando a implantação da sala segura modular interna, do POD de IA e de **2 (dois) PODs padrão**, incluindo os subsistemas de energia, climatização, *racks*, cabeamento, monitoramento, segurança, combate a incêndio, *moving* e certificação.

10.11.2. A Solução 2, baseada em *container*, deve ser comparada com o mesmo escopo funcional. Considerando a proporção de acréscimo anteriormente identificada entre a solução em *container* e a solução interna, estima-se valor mínimo comparativo de **R$ 66.650.000,00**, sem prejuízo de custos adicionais decorrentes da instalação externa e das interfaces com o *Data Center* existente.

10.11.3. As Soluções 3 e 4, embora possam reduzir investimento inicial em obras e infraestrutura própria, tendem a transferir custos para despesas recorrentes, contratos continuados, *links*, interconexões, suporte, migração, transporte, seguros, dependência operacional, expansão contratual, serviços gerenciados e eventuais custos de saída ou portabilidade.

10.11.4. A análise econômica não deve considerar apenas o menor desembolso inicial, mas o custo total de propriedade, a vida útil da infraestrutura, a capacidade institucional gerada, os riscos evitados, a redução de dependência externa, a preservação da soberania, o aproveitamento do sítio técnico existente e a inclusão dos **2 (dois) PODs padrão** no escopo global da solução.

10.11.5. Nesse sentido, a Solução 1 apresenta melhor custo-benefício preliminar, pois, mesmo com a ampliação do escopo para contemplar POD de IA e 2 (dois) PODs padrão, permanece mais integrada ao ambiente existente, gera capacidade institucional permanente, reduz dependência de terceiros e apresenta menor risco econômico quando comparada às alternativas de *container*, *colocation* e nuvem.

10.12. Resultado da análise comparativa:

10.12.1. A comparação das alternativas demonstra que a Solução 1 - Expansão da Sala Segura Modular dentro do DC RF - é a solução mais aderente ao interesse público e à necessidade institucional identificada neste Estudo Técnico Preliminar.

10.12.2. A Solução 1 apresenta maior aderência técnica, estratégica e operacional, pois permite ampliar a capacidade do *Data Center* Coronel Ricardo Franco em ambiente próprio e controlado, com suporte a alta densidade de IA, integração à infraestrutura existente, preservação da segurança física e lógica, manutenção da soberania dos dados, possibilidade de evolução tecnológica e compatibilidade com a certificação Tier III.

10.12.3. A Solução 2, embora tecnicamente possível e útil em cenários de implantação rápida ou contingencial, não demonstrou vantagem econômica nem maior aderência ao caráter permanente da expansão, além de ampliar a complexidade de segurança física e integração externa.

10.12.4. A Solução 3 pode ser útil como alternativa complementar, transitória ou contingencial, mas não atende plenamente à necessidade de controle soberano, capacidade institucional permanente e governança direta sobre o ambiente físico de processamento estratégico de IA.

10.12.5. A Solução 4, apesar de apresentar elasticidade e rapidez de provisionamento, não se mostra adequada como solução principal para cargas estratégicas de IA do Exército Brasileiro, em razão dos riscos de exposição de dados, metadados, artefatos de IA, dependência de provedor, restrições normativas e redução do controle institucional.

10.12.6. Conclui-se, portanto, que a solução mais vantajosa é a **Solução 1 - Expansão da Sala Segura Modular dentro do Data Center Coronel Ricardo Franco**, devendo as demais alternativas ser registradas como inviáveis ou não recomendadas como solução principal, sem prejuízo de eventual uso complementar, contingencial ou restrito, quando tecnicamente justificado e aprovado pela governança competente.

10.13. Solução recomendada:

10.13.1. Diante da análise comparativa realizada, recomenda-se a adoção da **Solução 1 - Expansão da Sala Segura Modular dentro do DC RF**, por ser a alternativa que melhor atende aos requisitos de segurança, soberania, disponibilidade, continuidade operacional, alta densidade computacional, integração com o ambiente existente, evolução tecnológica, economicidade preliminar e geração de capacidade institucional permanente.

10.13.2. A solução recomendada deverá ser desenvolvida por meio de projeto executivo detalhado, contemplando todos os subsistemas necessários à expansão do ambiente crítico, incluindo obras civis, Sala Segura, energia, UPS, grupos geradores, climatização, *chillers*, *in-row cooling*, *rear door heat exchangers*, rede passiva, monitoramento, controle de acesso, CFTV, combate a incêndio, *moving*, documentação *as built*, capacitação, suporte, recomposição das áreas afetadas e preservação da certificação Tier III.

10.13.3. A adoção da Solução 1 não impede que as demais alternativas venham a ser consideradas futuramente em hipóteses específicas, como contingência, expansão temporária, testes, cargas não sensíveis ou complementação de capacidade. Contudo, para o núcleo principal de processamento estratégico de Inteligência Artificial do Exército Brasileiro, a expansão interna da Sala Segura Modular no DC RF é a alternativa tecnicamente mais adequada, institucionalmente mais segura e economicamente mais vantajosa.

11. Registro de soluções consideradas inviáveis

11.1. Premissa geral da análise:

11.1.1. Nos termos da lógica do Estudo Técnico Preliminar, a escolha da solução deve decorrer da comparação entre alternativas possíveis, considerando viabilidade técnica, socioeconômica, ambiental, riscos, aderência à necessidade institucional e capacidade de atender ao interesse público. A IN SGD nº 94/2022 estabelece que o ETP deve evidenciar as necessidades de negócio e tecnológicas, os requisitos necessários e suficientes à escolha da solução de TIC, as alternativas de mercado, a declaração da viabilidade da contratação e a justificativa da solução escolhida.

11.1.2. No presente caso, a necessidade administrativa não se limita à simples disponibilização de capacidade computacional. Trata-se da expansão da capacidade operacional do *Data Center* Coronel Ricardo Franco para suportar cargas críticas, estratégicas e de alta densidade associadas ao processamento de inteligência artificial, com requisitos elevados de segurança física, segurança da informação, soberania de dados, continuidade operacional, auditabilidade, controle institucional e evolução tecnológica. O próprio estudo registra que a Solução 1 mantém a expansão dentro de infraestrutura própria do Exército, preservando controle físico, operacional e administrativo sobre o ambiente de processamento, além de favorecer integração com o sítio técnico, conectividade e governança já existentes no DC RF.

11.1.3. Dessa forma, as demais soluções, embora possam apresentar vantagens pontuais, não se mostram adequadas como solução principal e definitiva para o núcleo estratégico de processamento de IA do Exército Brasileiro.

11.2. Justificativa de inviabilidade da Solução 2 - Expansão modularizada do DC RF por *container*:

11.2.1. A solução de expansão por *container* consiste na implantação de módulos externos pré-fabricados, projetados para abrigar infraestrutura computacional crítica, com seus respectivos subsistemas de energia, climatização, segurança e monitoramento. Em tese, essa alternativa apresenta vantagens relacionadas à rapidez de implantação, modularidade, menor dependência de obras civis convencionais e possibilidade de realocação futura. Tais características podem ser úteis em cenários transitórios, emergenciais, de contingência ou de reforço temporário de capacidade. O estudo registra, inclusive, que o modelo em *container* tende a reduzir parte das intervenções civis e permite fabricação e integração parcial prévias. Todavia, no contexto específico da expansão do DC RF para processamento estratégico de IA, a solução por container não se mostra a mais adequada como solução principal, pelos fundamentos listados nesse item.

11.2.2. Menor aderência ao caráter permanente e estratégico da expansão:

11.2.2.1. A expansão pretendida não tem natureza transitória. O objetivo é estruturar uma capacidade permanente, institucional e evolutiva para processamento de IA, com aproveitamento do sítio já existente do *Data Center* Coronel Ricardo Franco e integração aos processos de segurança, operação, monitoramento, controle de acesso, conectividade e governança já consolidados.

11.2.2.2. Nesse aspecto, a solução em *container*, embora tecnicamente possível, caracteriza-se como alternativa menos integrada ao edifício principal do DC RF. Por ser instalada em área externa, ainda que adjacente ao *data center*, cria uma unidade física apartada do núcleo principal de processamento, com exigência de novos controles perimetrais, rotas de acesso, interfaces de energia, conectividade, drenagem, aterramento, proteção contra descargas atmosféricas, detecção e combate a incêndio, monitoramento e manutenção. O próprio estudo aponta que, apesar de reduzir parte das intervenções civis, a solução continua exigindo fundações, interligações elétricas, conectividade, drenagem, aterramento, SPDA, segurança perimetral e integração aos sistemas de incêndio e monitoramento.

11.2.2.3. Assim, a solução por *container* não elimina a complexidade de implantação, apenas desloca parte dela para interfaces externas e para a integração entre o *container* e a infraestrutura permanente do *data center*.

11.2.3. Exposição física ampliada e maior complexidade de segurança:

11.2.3.1. A instalação em área externa amplia a superfície de exposição do ambiente crítico. Ainda que o *container* permaneça em área controlada do Exército, sua localização fora do invólucro principal do *data center* aumenta a necessidade de medidas adicionais de segurança física, vigilância, controle de acesso, barreiras perimetrais, proteção contra intempéries, controle ambiental externo e planos específicos de resposta a incidentes.

11.2.3.2. Essa consideração é relevante porque a segurança da informação, conforme a IN GSI/PR nº 1 /2020, abrange não apenas segurança cibernética, mas também defesa cibernética, segurança física, proteção de dados organizacionais e ações destinadas a assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação.

11.2.3.4. No contexto de Defesa, essa exigência é ainda mais sensível. A Política para o Sistema Militar de Comando e Controle registra que os sistemas de TIC permeiam atividades operacionais e de apoio em todos os níveis de decisão e que são alvos prioritários no combate moderno, exigindo medidas de segurança para proteção das informações necessárias ao exercício do comando.

11.2.3.5. Portanto, embora o container possa ser protegido, ele impõe camada adicional de risco físico-operacional quando comparado à expansão interna de uma Sala Segura dentro do próprio DC RF, onde os controles físicos, operacionais e administrativos podem ser concebidos de forma mais integrada, permanente e auditável.

11.2.4. Limitações frente à evolução das cargas de IA:

11.2.4.1. As cargas de IA, especialmente aquelas associadas a servidores com GPU, treinamento de modelos, inferência em larga escala, processamento de dados sensíveis e operação de *clusters* de alto desempenho, tendem a exigir densidade elétrica e térmica superior à de ambientes tradicionais de TIC.

11.2.4.2. O cenário técnico atual confirma esse ponto. A Vertiv (fornecedora de infraestrutura digital crítica e soluções de continuidade para *data centers*, redes de comunicação e ambientes industriais/ comerciais) aponta que *data centers* voltados a IA e ML estão elevando densidades de *rack*, podendo alcançar patamares da ordem de 100 kW por *rack* em determinados ambientes, e que a implantação de refrigeração de alta densidade exige planejamento detalhado de carga térmica, vazão, disponibilidade de água gelada, CDU, redes secundárias de fluido, espaço técnico, tubulações, distribuição elétrica e monitoramento. O *Uptime Institute* também registra que, em 2025, poucas instalações superavam 30 kW por *rack*, o que demonstra que ambientes aptos a cargas muito densas ainda são exceção, não regra.

11.2.4.3. Nesse cenário, uma solução em *container* pode atender a determinada configuração inicial, mas tende a oferecer menor flexibilidade arquitetônica para evolução futura do que uma Sala Segura concebida dentro do *data center*. A expansão interna permite projetar o ambiente desde a origem para receber *racks* de alta densidade, refrigeração de precisão, *rear door heat exchangers*, *in-row cooling*, eventual refrigeração líquida, CDUs, distribuição elétrica robusta, rotas de cabeamento e espaços técnicos compatíveis com evolução tecnológica. Já o *container* fica mais condicionado à geometria, limites estruturais, capacidade térmica e arranjo proprietário do módulo adquirido.

11.2.5. Ausência de vantagem econômica demonstrada:

11.2.5.1. A solução por *container* também não demonstrou vantagem econômica em relação à Solução 1 quando comparada em escopo equivalente. Considerando o valor de referência atualizado da Solução 1, de **R$ 63.400.000,00**, e mantendo-se a proporção de acréscimo anteriormente observada na pesquisa preliminar, a solução por *container* passa a apresentar valor comparativo mínimo estimado de aproximadamente **R$ 66.650.000,00**.

11.2.5.2. Além de apresentar valor estimado superior ao da expansão interna, a Solução 2 conta com menor robustez na pesquisa de preços, pois se baseia em menor número de referências. Essa circunstância reduz a segurança da estimativa e pode demandar complementação de pesquisa de mercado em etapa posterior. Do ponto de vista da vantajosidade, não se justifica escolher solução mais onerosa, menos integrada e menos permanente, quando a Solução 1 aproveita área já existente no interior do DC RF, contempla POD de IA e 2 (dois) PODs padrão e gera capacidade institucional duradoura.

11.2.6. Conclusão quanto à Solução 2:

11.2.6.1. Diante do exposto, a solução de expansão modularizada por *container* deve ser considerada **inviável como solução principal e definitiva** para o processamento estratégico de IA no DC RF. Embora possa ser tecnicamente útil para cenários de contingência, reforço temporário, expansão emergencial ou capacidade complementar, ela apresenta menor aderência ao objetivo central da contratação, amplia a complexidade de segurança física, exige infraestrutura externa adicional, possui menor integração com o ambiente principal do *data center*, oferece menor flexibilidade para evolução de cargas de IA de alta densidade e não demonstrou vantagem econômica em relação à expansão interna da Sala Segura.

11.2.6.2. Assim, recomenda-se sua não adoção como solução escolhida, mantendo-a apenas como alternativa complementar ou contingencial em cenários futuros devidamente justificados.

11.3. Justificativa de inviabilidade da Solução 3 - *Colocation* de equipamentos:

11.3.1. A solução de *colocation* consiste na instalação de equipamentos de propriedade do Exército Brasileiro em *data center* pertencente e operado por terceiro, público ou privado, que passa a fornecer espaço físico, energia, climatização, conectividade, proteção contra incêndio e controles de segurança física. Nessa alternativa, os ativos de TI permanecem sob propriedade da Administração, mas a infraestrutura predial, os sistemas de suporte e parte relevante da operação ambiental passam a depender de terceiro. O estudo registra que essa solução pode apresentar vantagens de celeridade, redução de investimentos imediatos em obras civis e possibilidade de ampliação rápida de capacidade. Apesar dessas vantagens aparentes, a solução não se mostra adequada como alternativa principal para o núcleo estratégico de processamento de IA do Exército Brasileiro.

11.3.2. Redução do controle físico, operacional e administrativo:

11.3.2.1. O principal óbice do *colocation* está na redução do controle institucional sobre o ambiente físico de processamento. Ainda que os servidores, *storages*, *switches* e demais ativos permaneçam sob propriedade do Exército, eles passam a operar em ambiente externo, sujeito às regras, rotinas, políticas de acesso, manutenção, fiscalização, segurança, continuidade e disponibilidade do provedor de *colocation*.

11.3.2.2. Essa dependência é incompatível com a natureza do ambiente pretendido. O projeto busca estruturar capacidade própria de processamento de IA para cargas estratégicas, eventualmente associadas a dados sensíveis, informações restritas, sistemas de apoio à decisão, inteligência, operações, logística e comando e controle. Para tais cargas, não basta preservar a titularidade dos equipamentos; é necessário preservar também a governança física e operacional do ambiente onde os dados serão tratados.

11.3.2.3. A IN GSI/PR nº 1/2020 reforça que a segurança da informação deve assegurar disponibilidade, integridade, confidencialidade e autenticidade, abrangendo segurança cibernética, defesa cibernética, segurança física e proteção de dados organizacionais. No *colocation*, parte substancial desses controles passa a depender da contratada, reduzindo a capacidade de atuação direta da Administração sobre o ambiente de missão crítica.

11.3.3. Risco de exposição indireta da arquitetura tecnológica:

11.3.3.1. O *colocation* também aumenta a exposição indireta da arquitetura tecnológica do Exército. Mesmo quando há áreas segregadas, *cages* dedicados, controles biométricos, CFTV e registros de acesso, a operação em instalação de terceiro implica maior circulação de equipes externas, maior necessidade de "*remote hands*", maior dependência de rotinas do provedor e maior exposição de informações sobre topologia, densidade, consumo, padrões de redundância, janelas de manutenção, conectividade e requisitos operacionais.

11.3.3.2. No contexto militar, essas informações não são meramente acessórias. A Política para o Sistema Militar de Comando e Controle registra que sistemas de TIC são componentes essenciais das estruturas militares em crises e conflitos armados e, por isso, são alvos prioritários no combate moderno. Logo, a simples externalização física de componentes críticos pode ampliar riscos estratégicos, ainda que os dados estejam criptografados ou que os equipamentos permaneçam sob propriedade do Exército.

11.3.4. Incerteza quanto à capacidade de suportar IA de alta densidade:

11.3.4.1. O *colocation* somente seria tecnicamente aceitável se houvesse comprovação de que o provedor dispõe de infraestrutura apta a suportar as cargas de IA previstas, especialmente em termos de potência por *rack*, refrigeração, peso, redundância, conectividade, baixa latência, resiliência, segregação física e segurança.

11.3.4.2. Essa comprovação não pode ser presumida. Ambientes de IA e HPC exigem infraestrutura especializada. A NVIDIA, ao tratar de *data centers* de *colocation* aptos a plataformas DGX, destaca a necessidade de capacidade de alta densidade, experiência comprovada em *clusters* GPU e soluções avançadas de refrigeração por ar de alta densidade ou refrigeração líquida para suportar as demandas térmicas e elétricas de IA e HPC. O *Uptime Institute*, por sua vez, indica que poucas instalações superam 30 kW por rack, demonstrando que a oferta de *colocation* efetivamente preparada para cargas extremas de IA ainda é restrita.

11.3.4.3. O estudo também registra a necessidade de avaliação rigorosa da capacidade de *colocation* para suportar potência, peso, refrigeração, conectividade, segregação física e disponibilidade, especialmente porque cargas de IA podem demandar maior densidade elétrica e soluções avançadas de climatização.

11.3.5. Fragilidade como solução de longo prazo:

11.3.5.1. O *colocation* pode ser útil para contingência, expansão temporária, ambiente de recuperação de desastre, cargas menos sensíveis ou necessidades emergenciais. Entretanto, não gera capacidade institucional permanente. Ao final do contrato, permanece a dependência de renovação, renegociação, migração física dos equipamentos ou contratação de novo provedor. Também podem surgir custos de transporte, seguros, logística, instalação, desinstalação, interconexão, *links* dedicados, suporte remoto, *cross-connects*, expansão de energia, recomposição de *racks* e adequações específicas do provedor.

11.3.5.2. Além disso, em eventual situação de crise, restrição operacional, incidente de segurança, conflito contratual ou indisponibilidade do provedor, o Exército não teria o mesmo grau de autonomia que teria operando o ambiente dentro de seu próprio *data center*. Essa limitação contraria a finalidade estratégica do projeto, que é fortalecer a autonomia tecnológica e operacional do DC RF.

11.3.6. Limitações mesmo quando o provedor é empresa pública:

11.3.6.1. A existência de empresas públicas que ofertem serviços de hospedagem, *colocation* ou nuvem governamental não elimina a análise de aderência ao caso concreto. A Nuvem de Governo, por exemplo, foi estruturada para reforçar soberania digital, com operação pelo Serpro e Dataprev, dados em território nacional e conformidade com a legislação brasileira. Contudo, essa solução atende a um modelo de prestação de serviço governamental em nuvem ou hospedagem, não necessariamente ao escopo específico de implantação de uma capacidade própria, dedicada, *on-premise*, de alta densidade, controlada diretamente pelo Exército e voltada a cargas estratégicas de IA.

11.3.6.2. O estudo registra que, embora empresas públicas possam oferecer hospedagem ou computação em nuvem governamental, seus modelos de prestação de serviços e arquitetura não se mostram compatíveis com o escopo e a sensibilidade do projeto de IA do Exército, sobretudo quando o requisito central é o controle direto da infraestrutura e dos sistemas de TI.

11.3.7. Conclusão quanto à Solução 3:

11.3.7.1. Diante do exposto, a solução de colocation deve ser considerada **inviável como solução principal** para o núcleo estratégico de processamento de IA do Exército Brasileiro. Embora possa ser admitida em caráter complementar, transitório ou contingencial, ela reduz o controle físico, operacional e administrativo da Administração, amplia a dependência contratual, expõe indiretamente a arquitetura tecnológica, exige comprovação rigorosa de capacidade para alta densidade de IA e não gera capacidade institucional permanente no DC RF.

11.3.7.2. Assim, para a finalidade pretendida - expansão segura, soberana, duradoura e controlada da capacidade de processamento de IA - a Solução 1 apresenta maior aderência técnica, institucional e estratégica.

11.4. Justificativa de inviabilidade da Solução 4 - Hospedagem em nuvem:

11.4.1. A hospedagem em nuvem consiste na utilização de recursos computacionais sob demanda fornecidos por provedor externo, abrangendo, conforme o caso, IaaS, PaaS ou SaaS. A Portaria SGD/MGI nº 5.950/ 2023 define serviços de computação em nuvem como recursos físicos ou virtuais escaláveis, elásticos, compartilháveis, acessados via rede e administrados sob demanda, e estabelece o modelo de contratação aplicável aos órgãos do SISP.

11.4.2. Do ponto de vista técnico-operacional, a nuvem oferece vantagens conhecidas: elasticidade, provisionamento rápido, expansão sob demanda, ampla disponibilidade de serviços gerenciados e redução de investimento inicial em infraestrutura própria. Todavia, tais vantagens não são suficientes para caracterizá-la como solução adequada ao caso concreto, pois o objeto em análise envolve processamento estratégico de IA no âmbito do Exército Brasileiro, com dados e cargas de trabalho que podem exigir sigilo, restrição de acesso, soberania, segregação, auditabilidade e operação controlada.

11.4.3. Inadequação ao objeto pretendido:

11.4.3.1. A solução pretendida não é apenas a contratação de capacidade computacional genérica. O objetivo é implantar infraestrutura própria de IA no DC RF, abrangendo ambiente físico seguro, energia, refrigeração, *racks*, conectividade, suporte a alta densidade, operação local, governança institucional e possibilidade de processamento restrito.

11.4.3.2. A própria Portaria SGD/MGI nº 5.950/ 2023 diferencia o escopo de contratação de nuvem de outros objetos. O modelo abrange *software*, IaaS, PaaS, SaaS, suporte, migração, integração e gerenciamento de recursos em nuvem, mas expressamente não abrange aquisição de ativos de infraestrutura de TIC, aquisição de ativos de rede, *hosting* ou *colocation*.

11.4.3.3. Portanto, a nuvem não substitui integralmente o objeto pretendido, que é a criação de capacidade institucional própria, física e controlada para processamento de IA.

11.4.4. Classificação prévia da informação e restrições normativas:

11.4.4.1. A Portaria SGD/MGI nº 5.950/ 2023 estabelece que a estratégia de uso de *software* e computação em nuvem deve considerar requisitos de negócio, resultados pretendidos, segurança da informação, privacidade e especificidades de cada carga de trabalho. Também determina que o órgão submeta os dados à classificação prévia da informação, para assegurar que não haja restrições normativas ou legais ao tratamento em nuvem.

11.4.4.2. Esse ponto é decisivo. No caso do Exército Brasileiro, as cargas de IA podem envolver dados de inteligência, operações, logística, comando e controle, segurança cibernética, comunicações estratégicas, planejamento, sensores, bases corporativas e documentos com restrição de acesso. Assim, não é prudente tratar a nuvem pública ou híbrida como solução padrão.

11.4.4.3. A IN GSI/PR nº 8/2025, que dispõe sobre requisitos mínimos de segurança da informação para tratamento de informação classificada em computação em nuvem, admite o tratamento de informações classificadas em grau reservado ou secreto apenas em nuvem privada ou comunitária, com requisitos rigorosos, incluindo isolamento, criptografia com algoritmos de Estado, gestão exclusiva de chaves pelo órgão, autenticação multifator, *logs* imutáveis, controles de acesso, impedimento de acesso do provedor ao conteúdo e infraestrutura localizada em território nacional.

11.4.4.4. A mesma norma veda o tratamento em nuvem de informações classificadas em grau ultrassecreto e exige que informações reservadas ou secretas sejam armazenadas e processadas em *data centers* localizados exclusivamente em território nacional, vedando replicação ou *backup* fora do país.

11.4.4.5. Dessa forma, ainda que a nuvem possa ser utilizada para determinadas cargas públicas, não sensíveis ou de menor criticidade, ela não se apresenta como solução principal adequada para um ambiente de IA destinado a cargas estratégicas de Defesa.

11.4.5. Risco de exposição de dados, metadados e artefatos de IA:

11.4.5.1. Em ambientes de IA, a exposição potencial não se limita aos dados brutos. *Prompts*, bases de treinamento, vetores, *embeddings*, *logs*, parâmetros, metadados, pesos intermediários, modelos ajustados, resultados de inferência e padrões de uso podem revelar informações sensíveis sobre doutrina, logística, planejamento, capacidades, vulnerabilidades ou prioridades institucionais.

11.4.5.2. O presente estudo registra que a utilização de nuvem de terceiros para Soluções de Infraestrutura de IA foi descartada por representar risco à continuidade operacional e à integridade das informações de Defesa, além de apontar risco de que dados fornecidos a ferramentas de IA generativa possam ser utilizados para treinamento de modelos externos. Também registra que parecer técnico relativo ao EBOT apontou a infraestrutura *on-premise* como estado final desejado e solução definitiva para segurança da informação, mediante adaptação dos *Data Centers* Corporativos.

11.4.5.3. Ainda que provedores possam oferecer cláusulas contratuais, controles técnicos e ambientes segregados, a adoção de nuvem pública ou híbrida como solução principal implicaria dependência externa incompatível com a criticidade do objeto, especialmente quando o ambiente deve poder operar com elevado grau de autonomia, controle e restrição de acesso.

11.4.6. Dependência tecnológica, contratual e orçamentária:

11.4.6.1. A nuvem também gera dependência tecnológica e contratual significativa. O custo é normalmente baseado em consumo, reservas, armazenamento, tráfego de dados, saída de dados, serviços gerenciados, suporte e variação cambial. Em projetos de IA, essa dependência pode ser agravada pelo uso intensivo de GPU, armazenamento de grandes volumes de dados, movimentação de *datasets*, treinamento de modelos e necessidade de alta disponibilidade.

11.4.6.2. O estudo registra que, embora a nuvem possa apresentar menor CAPEX (*Capital Expenditure* - despesas de capitais) inicial, o OPEX (*Operational Expenditure* - despesas operacionais) tende a ser elevado e variável. Foi estimado custo de aproximadamente **R$ 550.000,00 por mês** para reserva de instâncias equivalentes ao núcleo de processamento de IA, o que, em 60 meses, superaria **R$ 33.000.000,00** apenas em computação. Todavia, essa estimativa não contempla integralmente o escopo ampliado da contratação, que inclui também **2 (dois) PODs padrão**. Considerando acréscimo mínimo de referência de **R$ 5.600.000,00** para esses PODs, o custo mínimo comparativo da alternativa em nuvem passaria a **R$ 38.600.000,00 milhões em 60 meses** e **R$ 71.600.000,00 em 120 meses**, ainda sem incluir armazenamento, tráfego de saída, suporte, licenciamento, serviços gerenciados, segurança, governança financeira, migração e custos de saída.

11.4.6.3. Além do custo direto, há riscos de imprevisibilidade orçamentária, dependência de moeda estrangeira, cobrança por saída de dados, dificuldade de portabilidade, *lock-in* tecnológico, custos de migração reversa e necessidade contínua de governança financeira especializada. Para orçamento público e planejamento militar, essa imprevisibilidade reduz a vantajosidade da solução.

11.4.7. Limitação para operação restrita ou desconectada:

11.4.7.1. Um dos requisitos estratégicos de um ambiente próprio de IA é a possibilidade de operação restrita, controlada e, quando necessário, isolada da internet pública. Esse requisito é relevante para cargas de Defesa, dados sensíveis e cenários de crise ou restrição operacional.

11.4.7.2. A nuvem pública, por definição, depende de infraestrutura externa, conectividade, disponibilidade do provedor, região contratada, regras de operação, políticas de acesso e continuidade do serviço externo. Embora existam arquiteturas híbridas e privadas, elas não eliminam integralmente a dependência de terceiros quando a solução principal é baseada em provedor externo.

11.4.7.3. Por essa razão, a solução *on-premise* no DC RF se mostra mais coerente com a necessidade de controle soberano, cadeia de custódia, segurança física, auditabilidade, autonomia operacional e possibilidade de segregação física do ambiente.

11.4.8. Nuvem de Governo não equivale automaticamente à solução pretendida:

11.4.8.1. A Nuvem de Governo representa avanço importante para soberania digital e armazenamento de dados sensíveis do Estado, sendo gerida pelo Serpro e Dataprev, com dados em território nacional e padrões de segurança e operação. Contudo, ela não substitui automaticamente a necessidade de infraestrutura própria para processamento estratégico de IA do Exército.

11.4.8.2. A própria existência da Nuvem de Governo reforça que dados sensíveis demandam tratamento diferenciado, governança reforçada e maior controle estatal. Entretanto, para o caso concreto do DC RF, o requisito não é apenas hospedar dados sensíveis em ambiente governamental, mas estruturar capacidade própria, dedicada, permanente e evolutiva para processamento de IA, com domínio direto do ambiente físico, da arquitetura, da operação, da expansão elétrica e térmica e dos controles de segurança.

11.4.8.3. Assim, a Nuvem de Governo pode ser considerada, em tese, para cargas específicas, acessórias, públicas, não sensíveis ou complementares, desde que observada a estratégia institucional de uso de nuvem e a classificação da informação. Não se mostra, contudo, substituta integral da expansão da Sala Segura do DC RF.

11.4.9. Conclusão quanto à Solução 4:

11.4.9.1. Diante do exposto, a hospedagem em nuvem deve ser considerada **inviável como solução principal** para a sustentação das Soluções de Infraestrutura de IA do Exército Brasileiro no contexto do DC RF. A alternativa não atende plenamente aos requisitos de soberania, controle físico, cadeia de custódia, previsibilidade orçamentária, operação restrita, processamento de cargas sensíveis e formação de capacidade institucional permanente.

11.4.9.2. Sua utilização pode ser admitida apenas de forma complementar, controlada e restrita, para cargas sem restrição de acesso, ambientes de desenvolvimento, testes, dados públicos, serviços acessórios ou hipóteses aprovadas pela governança competente, sempre precedida de classificação da informação, análise de riscos, estratégia de uso de nuvem e conformidade com a Portaria SGD/MGI nº 5.950/ 2023 e com as normas do GSI.

11.5. Assim, a Solução 1 - **expansão da Sala Segura Modular dentro do DC RF** - mostra-se a alternativa mais aderente ao interesse público, por combinar aproveitamento de área já existente, fortalecimento da infraestrutura própria, maior controle institucional, melhor integração com a operação atual do data center, maior compatibilidade com cargas críticas de IA e maior alinhamento com os requisitos de segurança, soberania e continuidade operacional do Exército Brasileiro.

12. Análise comparativa de custos (TCO)

12.1. Considerações:

12.1.1. A análise comparativa de custos das soluções foi realizada com base no conceito de Custo Total de Propriedade - *Total Cost of Ownership* (TCO), considerando o custo inicial de implantação, os custos recorrentes de manutenção, os custos indiretos associados à operação, os riscos econômicos de dependência de terceiros e a capacidade de geração de ativo institucional permanente para o Exército Brasileiro, em consonância com o Plano Diretor de Logística Sustentável do 7º CTA.

12.1.2. A comparação econômica deve ser interpretada em conjunto com a análise técnica das soluções, uma vez que a presente contratação não se refere à simples aquisição de capacidade computacional genérica, mas à estruturação de ambiente crítico de *data center*, apto a hospedar cargas de Inteligência Artificial de alta

densidade, com requisitos de segurança física, segurança da informação, continuidade operacional, soberania de dados, disponibilidade e aderência à certificação Tier III.

12.1.3. Para fins de análise, foram consideradas as quatro soluções levantadas no estudo: Solução 1 - expansão da Sala Segura Modular dentro do DC RF; Solução 2 - expansão modularizada por *container*; Solução 3 - *colocation* de equipamentos; e Solução 4 - hospedagem em nuvem.

12.1.4. Como horizonte de avaliação, adotou-se o período de 10 anos, compatível com a natureza da infraestrutura crítica de *data center*, com os ciclos de vida típicos de sistemas elétricos, climatização, monitoramento, segurança física, *racks*, cabeamento, subsistemas de apoio e demais componentes de infraestrutura.

12.1.5. Para as simulações que dependem de conversão cambial, utilizou-se, apenas como referência comparativa, a taxa de câmbio comercial de compra de R$ 5,0071/US$, indicada na série histórica do Ipeadata para 21 de maio de 2026. Tal referência não substitui a cotação a ser utilizada em eventual pesquisa formal de preços ou contratação futura, servindo apenas para comparação econômica preliminar com dados internacionais.

12.2. Referências externas de mercado para contextualização dos custos:

12.2.1. A análise de custos deve considerar que o mercado global de *data centers* vem apresentando elevação relevante de preços, especialmente em razão da demanda por IA, da escassez de capacidade elétrica, do aumento da densidade por *rack*, da necessidade de climatização especializada e da maior complexidade dos sistemas mecânicos e elétricos.

12.2.2. Segundo a JLL (*Jones Lang LaSalle* - consultoria global especializada no mercado de imóveis comerciais e corporativos) o custo médio global de construção de *data centers* aumentou de US$ 7,7 milhões por MW em 2020 para US$ 10,7 milhões por MW em 2025, com previsão de alcançar US$ 11,3 milhões por MW em 2026. A mesma fonte ressalta que esses valores se referem ao *shell and core* da construção, sendo que o *fit-out* tecnológico para infraestrutura de IA pode atingir até US$ 25 milhões por MW.

12.2.3. A *Turner & Townsend* (consultora em ativos e construção) aponta que *data centers* de maior densidade, com resfriamento líquido e voltados a cargas de IA, apresentam prêmio médio de construção entre 7% e 10% em relação a *data centers* equivalentes refrigerados a ar, em razão da maior complexidade dos sistemas técnicos, mecânicos e de refrigeração.

12.2.4. O *Uptime Institute*, em seu *Global Data Center Survey* 2025, registra que mais de 80% dos operadores pesquisados não possuem *racks* acima de 30 kW, e que *racks* acima de 100 kW ainda são raros. Esse dado reforça que ambientes capazes de suportar *racks* de 65 kVA, como previsto neste ETP, não correspondem a *data centers* convencionais, mas a ambientes especializados de alta densidade.

12.2.5. Tais referências demonstram que a expansão pretendida pelo DC RF, com capacidade de planejamento de até 800 kW para ambiente de IA, encontra-se alinhada a uma tendência internacional de crescimento de custos para infraestruturas críticas de alta densidade, especialmente aquelas voltadas a IA, HPC e processamento acelerado por GPU.

12.3. Custo da Solução 1 - Expansão da Sala Segura Modular dentro do DC RF:

12.3.1. A Solução 1 consiste na expansão da capacidade do *Data Center* Coronel Ricardo Franco por meio da implantação de Sala Segura Modular em área técnica já existente no interior do próprio edifício do *Data Center*, aproveitando espaço previamente concebido para expansão e mantendo o novo ambiente dentro do sítio físico, lógico e operacional controlado pelo Exército Brasileiro.

12.3.2. Para fins de estimativa da contratação, a Solução 1 possui valor global de referência de **R$ 63.373.755,45**, adotando-se, para fins de planejamento orçamentário, o valor arredondado de **R$ 63.400.000,00** .

12.3.3. O valor estimado contempla a implantação integrada da Sala Segura Modular, do POD de IA e de **2 (dois) PODs padrão**, incluindo estrutura, climatização, *nobreaks*/ UPS adicionais, *racks*, adequações elétricas,

cabeamento, monitoramento, segurança, combate a incêndio, *moving*, certificação e demais componentes necessários à operação integrada do ambiente.

12.3.4. Considerando que a análise de TCO anteriormente adotava custo acumulado de manutenção preditiva e corretiva equivalente a aproximadamente 32,8% do valor de implantação, a aplicação da mesma proporção ao novo valor de referência resulta em custo estimado de manutenção da ordem de **R$ 20.800.000,00** ao longo do horizonte analisado.

12.3.5. Assim, para fins de comparação em ciclo de vida, o TCO decenal estimado da Solução 1 passa a ser de aproximadamente **R$ 84.200.000,00**, composto pelo valor de referência da contratação de **R$ 63.400.000,00** e pela estimativa proporcional de manutenção ao longo do período.

Componente	Valor estimado
Valor de referência da contratação - POD de IA + 2 PODs padrão	R$ 63.400.000,00
Manutenção estimada no horizonte decenal	R$ 20.800.000,00
TCO decenal estimado	**R$ 84.200.000,00**

12.3.6. Considerando a nova carga de TI adicionada de aproximadamente **1.130 kW**, resultante do POD de IA de 800 kW acrescido de 2 (dois) PODs padrão de 165 kW cada, o valor de referência da contratação corresponde a aproximadamente **R$ 56.106,19/kW** de carga de TI adicional.

12.3.7. A Solução 1, embora demande investimento inicial relevante, apresenta maior aderência econômica ao interesse público por gerar capacidade institucional permanente, aproveitar área já existente no DC RF, reduzir dependência de terceiros, preservar a soberania dos dados e permitir amortização do investimento ao longo de múltiplos ciclos tecnológicos.

12.4. Custo da Solução 2 - Expansão modularizada por *container*:

12.4.1. A Solução 2 consiste na implantação de data center modular do tipo *container* em área externa adjacente ao edifício do DC RF, com seus respectivos subsistemas de energia, climatização, monitoramento, segurança e interconexão.

12.4.2. Para fins de comparação econômica, a Solução 2 deve ser analisada em escopo equivalente ao da Solução 1, contemplando o POD de IA e os 2 (dois) PODs padrão. Considerando que, na pesquisa preliminar, a solução por *container* apresentou valor aproximadamente **5,11%** superior à solução interna, aplica-se essa mesma proporção ao novo valor de referência da Solução 1. Dessa forma, obtém-se valor comparativo mínimo estimado de **R$ 66.650.000,00** para a Solução 2.

12.4.3. A tabela a seguir apresenta a comparação preliminar entre Solução 1 e Solução 2:

Solução	Base de comparação	Valor preliminar atualizado
Solução 1 - Sala Segura Modular interna com POD de IA e 2 PODs padrão	Valor de referência da contratação	R$ 63.400.000,00
Solução 2 - *Container* em escopo equivalente	Acréscimo proporcional de 5,11%	R$ 66.650.000,00
Diferença estimada da Solução 2 em relação à Solução 1	-	R$ 3.250.000,00

12.4.4. A análise de custo da Solução 2 deve considerar que o valor cotado para o *container* não encerra, necessariamente, todos os custos de implantação em ambiente de missão crítica. Por estar instalado em área externa, o *container* tende a exigir fundações, bases, interligações elétricas e lógicas, SPDA, aterramento, drenagem, segurança perimetral, proteção contra intempéries, controle de acesso, monitoramento, integração com sistemas de incêndio, recomposição externa, rotas de cabos e eventual adequação de caminhos físicos entre o *container* e o *data center* existente.

12.4.5. Além disso, a cotação única reduz a robustez da estimativa econômica, pois não permite aferir adequadamente a variação de mercado, a composição dos custos, a equivalência de escopo e a aderência integral aos requisitos de alta densidade, certificação Tier III, segurança física e evolução tecnológica para cargas de IA.

12.4.6. A pesquisa externa de mercado reforça que *data centers* de IA possuem custos adicionais relevantes, especialmente quando demandam maior densidade, sistemas técnicos mais complexos e eventual adoção de refrigeração líquida. A *Turner & Townsend* indica prêmio médio de 7% a 10% para *data centers* de maior densidade com resfriamento líquido em comparação com soluções equivalentes refrigeradas a ar.

12.4.7. Dessa forma, mesmo que a Solução 2 possa oferecer vantagens pontuais de modularidade e velocidade de implantação, ela não demonstrou vantagem econômica em relação à Solução 1. Ao contrário, apresentou maior custo preliminar, menor robustez de pesquisa, maior exposição física externa e maior incerteza quanto aos custos indiretos de integração, segurança e operação ao longo do ciclo de vida.

12.5. Custo da Solução 3 - *Colocation* de equipamentos:

12.5.1. A Solução 3 consiste na instalação de equipamentos do Exército em *data center* de terceiro, mediante contratação de espaço físico, energia, climatização, conectividade, segurança e serviços associados.

12.5.2. A vantagem econômica aparente do *colocation* está na redução do investimento inicial em infraestrutura própria. Entretanto, essa solução converte o custo de implantação em despesa recorrente, geralmente calculada por kW/mês, acrescida de custos de conectividade, *cross-connects*, suporte remoto, serviços gerenciados, seguro, transporte, migração, expansão contratual e eventual saída do ambiente contratado.

12.5.3. Como referência de mercado, a CBRE (*Coldwell Banker Richard Ellis* - empresa de serviços e investimentos imobiliários comerciais) registrou, no relatório *North America Data Center Trends* H2 2025, o valor médio de US$ 196,25/kW/mês para demandas de 250 kW a 500 kW em mercados primários de *wholesale colocation*. A mesma fonte indica que a competição por grandes blocos de capacidade contígua e energia escalável elevou os preços em requisitos de maior porte.

12.5.4. Em outra referência de mercado, o relatório *Global Data Center Trends* 2025 aponta preços globais de *data center* na ordem de US$ 217,30/kW/mês no primeiro trimestre de 2025, com pressão de demanda decorrente de IA, *cloud* e restrições de capacidade elétrica.

12.5.5. Aplicando-se esses valores de referência à carga de planejamento atualizada de **1.130 kW**, correspondente ao POD de IA e aos 2 (dois) PODs padrão, obtém-se o seguinte exercício comparativo, sem incluir aquisição de *hardware* de IA, *storages*, *switches*, licenças, seguros, interconexões, *links* dedicados, serviços gerenciados, suporte adicional, custos de saída, migração reversa ou requisitos específicos de segurança militar.

12.5.6. A tabela a seguir apresenta uma simulação referencial de custo de *colocation* para 800 kW:

Referência de mercado	Custo mensal estimado	Custo anual estimado	Custo em 10 anos
US$ 196,25/kW/mês	R$ 1.110.387,01	R$ 13.324.644,17	R$ 133.246.441,65
US$ 217,30/kW/mês	R$ 1.229.488,40	R$ 14.753.860,77	R$ 147.538.607,75

12.5.7. Observa-se que, no horizonte de 10 anos, a contratação de *colocation* para **1.130 kW** poderia atingir valor referencial entre **R$ 133.250.000,00 e R$ 147.540.000,00**, sem formação de ativo institucional próprio e sem incluir diversos custos acessórios indispensáveis à operação. Em comparação, o valor de referência da Solução 1 é de **R$ 63.400.000,00**, e seu TCO decenal estimado, quando considerada manutenção proporcional, é de aproximadamente **R$ 84.200.000,00**.

12.5.8. Além do custo recorrente elevado, há limitação relevante de oferta técnica. O *Uptime Institute* registra que mais de 80% dos operadores pesquisados não possuem *racks* acima de 30 kW, enquanto o ambiente previsto no ETP requer suporte a *racks* de até 65 kVA, demonstrando que a disponibilidade de *colocation* verdadeiramente apto a IA de alta densidade é restrita.

12.5.9. Assim, a Solução 3 pode ser economicamente considerada apenas para situações complementares, transitórias ou contingenciais, mas não se mostra mais vantajosa que a expansão própria do DC RF quando analisados o custo decenal, a ausência de formação de ativo permanente, a dependência de terceiros e a incerteza de oferta local compatível com alta densidade de IA.

12.6. Custo da Solução 4 - Hospedagem em nuvem:

12.6.1. A Solução 4 consiste na utilização de recursos computacionais em nuvem, sob demanda ou mediante reserva, por meio de provedor externo. Essa alternativa reduz o CAPEX inicial de infraestrutura física, mas transfere o custo para modelo recorrente de consumo, normalmente vinculado a instâncias de GPU, armazenamento, tráfego de dados, saída de dados, suporte, licenciamento, serviços gerenciados, reserva de capacidade e variação cambial.

12.6.2. O próprio estudo registra estimativa de aproximadamente R$ 550.000,00 por mês para reserva de instâncias equivalentes, o que resulta em R$ 33.000.000,00 em 60 meses e R$ 66.000.000,00 em 120 meses, apenas em computação, sem incluir armazenamento, tráfego de saída, suporte, serviços gerenciados, segurança, licenciamento, governança financeira e custos de migração.

12.6.3. Como *benchmark* externo, a AWS (*Amazon Web Services* - plataforma de computação em nuvem amplamente adotada em nível mundial) informa que instâncias P5 utilizam até 8 GPUs NVIDIA H100 por instância e são voltadas a *deep learning*, IA generativa e HPC. A página oficial de *Capacity Blocks* da AWS apresenta exemplo de preço efetivo de US$ 31,464 por hora para instância p5.48xlarge na região *US East (Ohio)*.

12.6.4. Considerando, apenas para fins comparativos, uma configuração mínima de 48 GPUs H100, seriam necessárias 6 instâncias de 8 GPUs. Aplicando-se o valor de US$ 31,464/hora por instância, a operação contínua 24x7 alcançaria aproximadamente R$ 690.040,07 por mês, R$ 8.280.480,81 por ano e R$ 82.804.808,10 em 10 anos, apenas para a reserva computacional, sem armazenamento, tráfego de saída, suporte, licenças, serviços gerenciados ou custos de segurança.

12.6.5. Como referência adicional, a *Google Cloud* documenta que a máquina a3-highgpu-8g possui 8 GPUs NVIDIA H100, 208 vCPUs, 1.872 GB de memória, 6.000 GiB de SSD local e até 1.000 Gbps de largura de banda. Consulta pública de mercado para esse tipo de instância indica preço aproximado de US$ 88,49/hora para a máquina a3-highgpu-8g, o que, em configuração equivalente de 48 GPUs, resultaria em custo mensal aproximado de R$ 1.940.682,86 e custo decenal aproximado de R$ 232.881.943,44, apenas em computação.

12.6.6. A *Microsoft* também caracteriza a série *Azure* ND H100 v5 como voltada a treinamento avançado de *Deep Learning*, IA generativa e HPC, com uma VM iniciando em 8 GPUs NVIDIA H100 e possibilidade de escalonamento para milhares de GPUs, com 3,2 Tbps de largura de banda de interconexão por VM. Essa referência demonstra que cargas equivalentes às pretendidas exigem instâncias especializadas de alto desempenho, normalmente associadas a custos elevados e dependência de disponibilidade de capacidade nos provedores.

12.6.7. A tabela a seguir apresenta uma simulação referencial de custo de nuvem para 48 GPUs H100 em operação contínua:

Referência	Custo mensal estimado	Custo anual estimado	Custo em 5 anos	Custo em 10 anos ajustado ao escopo mínimo
Estimativa interna do estudo - R$ 550.000,00/mês para núcleo de IA	R$ 550.000,00	R$ 6.600.000,00	R$ 33.000.000,00	R$ 71.600.000,00
AWS p5.48xlarge Capacity Block - US$		R$	R$	

31,464/h por instância	R$ 690.040,07	8.280.480,81	41.402.404,05	R$ 88.404.808,10
Google Cloud a3-highgpu-8g - US$ 88,49 /h por instância	R$ 1.940.682,86	R$ 23.288.194,34	R$ 116.440.971,72	R$ 238.481.943,44

12.6.8. A simulação demonstra que a nuvem pode apresentar custo inicial reduzido, mas possui OPEX elevado e sensível ao tempo de uso, à disponibilidade de instâncias, à moeda estrangeira, ao tipo de reserva, ao tráfego de dados, ao armazenamento e aos serviços complementares. Mesmo na estimativa interna mais conservadora, a operação contínua em nuvem, acrescida de referência mínima para os 2 (dois) PODs padrão, alcançaria **R$ 71.600.000,00 em 10 anos**, apenas como piso comparativo, sem contemplar integralmente armazenamento, tráfego de saída, suporte, licenciamento, segurança, governança, migração e custos de saída.

12.6.9. Ademais, o custo de nuvem não gera ativo institucional permanente, não amplia a infraestrutura própria do DC RF, não preserva o mesmo nível de controle físico e operacional e pode gerar dependência tecnológica, contratual e orçamentária. Por essa razão, a nuvem pode ser economicamente justificável para cargas temporárias, testes, desenvolvimento, dados públicos ou ambientes complementares, mas não se mostra mais vantajosa como solução principal para sustentação contínua de cargas estratégicas de IA.

12.7. Matriz comparativa consolidada de custos das soluções:

Solução	CAPEX inicial estimado	OPEX/ TCO estimado	Comparação econômica	Observações
Solução 1 - Sala Segura Modular interna + POD de IA + 2 PODs padrão	R$ 63.400.000,00	R$ 84.200.000,00 em 10 anos, com manutenção proporcional estimada	Melhor relação entre custo, permanência do ativo, segurança e controle institucional	Gera ativo próprio, aproveita área existente, contempla POD de IA e 2 PODs padrão e reduz dependência externa
Solução 2 - *Container*	R$ 66.650.000,00, em escopo equivalente mínimo	TCO completo não demonstrado com robustez	Não demonstrou vantagem econômica sobre a Solução 1	Valor mínimo estimado superior, com maior incerteza de custos indiretos de implantação externa
Solução 3 - *Colocation*	Menor CAPEX próprio	Referência entre R$ 133.250.000,00 e R$ 147.540.000,00 em 10 anos para 1.130 kW	Tende a superar o TCO da Solução 1 no horizonte decenal	Não gera ativo permanente e depende de oferta de alta densidade por terceiro
Solução 4 - Nuvem	Menor CAPEX próprio	De R$ 71.600.000,00 a R$ 238.480.000,00 em 10 anos, conforme *benchmark* utilizado	Custo recorrente elevado e variável	Não gera ativo próprio e possui risco de variação cambial, *egress*, *lock-in* e dependência de provedor

12.8. Conclusão da análise comparativa de custos:

12.8.1. A análise comparativa de custos demonstra que a Solução 1 - expansão da Sala Segura Modular dentro do DC RF - apresenta a melhor relação entre custo total, benefício institucional, controle operacional, soberania, segurança e formação de capacidade permanente para o Exército Brasileiro.

12.8.2. A Solução 2, embora possa apresentar vantagens de modularidade e implantação acelerada, não demonstrou vantajosidade econômica em relação à Solução 1. Em escopo equivalente, contemplando POD de IA e 2 (dois) PODs padrão, a solução por *container* apresenta valor comparativo mínimo estimado de **R$ 66.650.000,00**, superior ao valor de referência da Solução 1, além de não evidenciar, com a mesma robustez, todos os custos indiretos de implantação externa, segurança perimetral, interligações, monitoramento, proteção contra intempéries, manutenção e integração com o DC RF.

12.8.3. A Solução 3, baseada em *colocation*, reduz a necessidade de investimento inicial próprio, mas gera despesa recorrente elevada. A simulação com referências internacionais de mercado indica custo decenal entre **R$ 133.250.000,00 e R$ 147.540.000,00 para 1.130 kW**, sem incluir diversos custos acessórios e sem formação de ativo institucional permanente. Além disso, a oferta de *colocation* apto a *racks* de 65 kVA é restrita, pois a maior parte dos *data centers* de mercado não opera com densidades superiores a 30 kW por *rack*.

12.8.4. A Solução 4, baseada em nuvem, apresenta elasticidade e baixo CAPEX inicial, mas o custo recorrente de instâncias de GPU em operação contínua é elevado e variável. Mesmo na estimativa interna mais conservadora, quando considerado acréscimo mínimo para contemplar os 2 (dois) PODs padrão, o custo em 10 anos alcança **R$ 71.600.000,00**, enquanto *benchmarks* públicos de mercado para 48 GPUs H100, acrescidos do mesmo ajuste mínimo de escopo, podem superar **R$ 88.000.000,00 ou R$ 238.000.000,00 em 10 anos**, conforme o provedor e a modalidade de contratação considerados.

12.8.5. Portanto, sob a ótica do Custo Total de Propriedade, da previsibilidade orçamentária, da redução de riscos econômicos, da soberania dos dados, da segurança da informação e da geração de ativo permanente, conclui-se que a Solução 1 permanece como a alternativa economicamente mais adequada para o atendimento da necessidade administrativa.

12.8.6. A adoção da Solução 1 permite que o investimento realizado permaneça incorporado ao patrimônio tecnológico do Exército Brasileiro, ampliando de forma duradoura a capacidade do *Data Center* Coronel Ricardo Franco para hospedar cargas críticas de Inteligência Artificial, com menor dependência de provedores externos e maior aderência aos requisitos estratégicos de Defesa, disponibilidade, continuidade operacional e controle institucional.

13. Descrição da solução de TIC a ser contratada

13.1. A solução a ser contratada refere-se à **Instalação de Sala Segura na área de expansão Data Center Ricardo Franco**, conforme será descrita nos itens subsequentes.

13.2. Expansão interna da Sala Segura em área já existente:

13.2.1. A primeira decisão relevante quanto a Solução 1 é a utilização da área de expansão existente no próprio DC RF, em vez da construção de um novo ambiente externo, da adoção de *container*, da contratação de colocation ou da hospedagem em nuvem.

13.2.2. A expansão contempla uma Sala Segura de aproximadamente **130 m²**, em área técnica já prevista no projeto original, destinada à implantação de ambiente de alta densidade para processamento de IA. O ambiente será otimizado para acomodar um POD de *racks* de alta densidade, composto por **12 (doze) racks de TI com densidade térmica de até 65 kW por *rack***, além de **2 (dois) *racks* de Telecom**, com carga total estimada na ordem de **800 kW**.

13.2.3. Essa escolha é tecnicamente mais adequada porque aproveita um espaço já integrado ao *data center*, reduzindo a necessidade de criação de um novo sítio operacional e permitindo a expansão dentro do perímetro físico e lógico já controlado. A solução preserva a unidade do ambiente crítico, facilita o controle de acesso, simplifica a integração com telecomunicações, energia, monitoramento, combate a incêndio, segurança patrimonial e operação assistida, além de reduzir a exposição física em comparação com alternativas externas.

13.2.4. Em comparação com a solução por *container*, a Sala Segura interna apresenta maior caráter permanente e maior aderência ao conceito de infraestrutura institucional estratégica, além do projeto original já considerar uma área de expansão justamente para este tipo de necessidade. O container poderia oferecer maior rapidez de implantação, mas traria maior exposição física por estar em área externa, maior dependência de interfaces civis, elétricas e de segurança perimetral, além de menor integração com o núcleo principal do DC RF.

13.2.5. Portanto, a escolha da expansão interna da Sala Segura decorre da combinação de 5 (cinco) fatores principais: (1) aproveitamento de área já existente; (2) preservação da soberania sobre dados e ativos; (3) maior integração com o ambiente atual; (4), menor exposição física; e (5) maior aderência à formação de capacidade permanente de IA no âmbito do Exército Brasileiro.

13.3. Arquitetura de geração de energia com 4 (quatro) geradores de 1 MVA em configuração N+1:

13.3.1. A segunda questão relevante da Solução 1 diz respeito à arquitetura de geração de energia.

13.3.2. Atualmente, o DC RF conta com dois grupos geradores de 1 MVA. A solução escolhida prevê a instalação de mais 2 (dois) grupos geradores de 1 MVA, totalizando 4 (quatro) unidades, que operarão em paralelo no regime **3 + 1**, isto é, 3 (três) geradores compondo a capacidade ativa de geração e 1 (um) gerador de reserva, caracterizando arquitetura **N+1**. Dessa forma, a instalação passará a contar com capacidade máxima de geração de **3 MVA**, com uma unidade redundante para manutenção, indisponibilidade programada ou falha de componente.

13.3.3. Essa decisão foi adotada após avaliação de alternativa mais robusta, baseada em configuração **2N**, com duas linhas independentes, cada uma com aproximadamente 2,5 MVA, o que demandaria a instalação de geradores de maior porte, notadamente unidades de 1,5 MVA em cada linha existente. Embora a arquitetura 2N apresente elevado grau de redundância, sua adoção, neste caso específico, não se mostrou a alternativa mais proporcional, econômica e tecnicamente adequada.

13.3.4. O principal fator limitador é estrutural. A laje técnica possui capacidade de carga limitada e conta com dois *slots* de expansão concebidos no mesmo padrão dos geradores atuais, compatíveis com equipamentos de 1 MVA. A adoção de geradores de 1,5 MVA implicaria maior peso, maior esforço estrutural, maior complexidade de içamento e instalação, maior demanda de adequações civis e maior risco técnico para a laje existente. Considerando que a laje sustenta 150 kg/m², a escolha por geradores de 1 MVA reduz o risco estrutural e aproveita o padrão de expansão já previsto.

13.3.5. Além do aspecto estrutural, a solução com 4 (quatro) geradores de 1 MVA é mais racional sob o ponto de vista econômico e operacional. Geradores de 1 MVA tendem a ser mais compatíveis com a infraestrutura existente, mais simples de integrar ao sistema de paralelismo, mais aderentes aos *slots* já disponíveis, mais baratos em relação à alternativa com unidades de 1,5 MVA e mais adequados à estratégia de certificação Tier III.

13.3.6. A *Uptime Institute* define o Tier III como uma instalação "*concurrently maintainable*", isto é, com componentes redundantes e caminhos de distribuição redundantes, permitindo que componentes e caminhos sejam retirados para manutenção planejada sem impacto à operação. Assim, a certificação Tier III não exige, por si só, que toda a geração seja necessariamente em 2N, mas exige que a arquitetura global permita manutenção concorrente dos componentes e caminhos críticos sem interrupção da carga de TI. A configuração N+1 com paralelismo, quando corretamente integrada aos sistemas de distribuição, UPS, chaveamento e automação, mostra-se compatível com essa diretriz de disponibilidade, desde que o projeto final seja validado conforme os critérios da *Uptime Institute*.

13.3.7. Portanto, a escolha pela configuração **3 + 1 com geradores de 1 MVA** representa a alternativa mais equilibrada entre disponibilidade, custo, risco estrutural, compatibilidade com a infraestrutura existente e possibilidade de certificação Tier III. A alternativa 2N com geradores de 1,5 MVA, embora tecnicamente superior em redundância bruta, foi afastada por impor maior peso, maior custo, maior complexidade de implantação e maior risco estrutural, sem que tais acréscimos fossem indispensáveis ao objetivo de certificação Tier III e à necessidade operacional do DC RF.

13.4. POD de IA de alta densidade com 12 *racks* de TI e 2 *racks* de Telecom:

13.4.1. Um terceiro ponto é a implantação de um POD dedicado ao processamento de IA, composto por **12 (doze) *racks* de TI de alta densidade**, com até **65 kW por *rack***, mais **2 (dois) racks de Telecom**, totalizando aproximadamente **800 kW** de carga instalada.

13.4.2. Essa escolha decorre da natureza das cargas de trabalho de IA. Servidores acelerados por GPU, *clusters* de treinamento, inferência em larga escala, *storages* de alto desempenho e redes de baixa latência exigem densidades elétricas e térmicas superiores às de *data centers* corporativos tradicionais. A literatura técnica atual confirma que cargas de IA e HPC tem levado *data centers* a densidades de *rack* muito elevadas, podendo atingir patamares da ordem de 100 kW por *rack* em determinados cenários, tornando indispensável o uso de soluções avançadas de resfriamento de alta densidade.

13.4.3. Dessa forma, a adoção de um POD específico para IA permite concentrar, controlar e monitorar a carga de maior criticidade dentro da Sala Segura, em vez de distribuí-la de forma difusa pelo *data hall*. Essa abordagem facilita a segregação física, o controle térmico, o balanceamento elétrico, o monitoramento ambiental, a gestão de capacidade, o cabeamento estruturado, a manutenção e a futura evolução tecnológica.

13.4.4. A solução também preserva flexibilidade para crescimento. O texto técnico prevê, além do POD principal de IA, a possibilidade de implantação de PODs complementares, com carga média inferior, destinados a acomodar outros conjuntos de *racks*, ampliando a capacidade do DC RF de maneira modular.

13.4.5. Em comparação com uma expansão convencional por *racks* distribuídos, a adoção de POD dedicado é mais adequada porque cria um domínio técnico específico para cargas de IA. Em comparação com a aquisição imediata de um ambiente integralmente *liquid cooling*, a solução escolhida é mais prudente, pois permite iniciar com arquitetura *air cooling* de alta capacidade, complementada por tecnologias preparadas para migração parcial ou total para *liquid cooling* quando a composição real dos servidores assim exigir.

13.5. Solução híbrida de resfriamento: *Rear Door Heat Exchanger* + *In-Row*:

13.5.1. A quarta abordagem foi sobre a escolha de uma arquitetura de resfriamento híbrida para o POD de IA, combinando ***Rear Door Heat Exchangers* - RDHx** nas portas traseiras dos *racks* com unidades ***In-Row*** de climatização de precisão.

13.5.2. A lógica técnica é a seguinte: cada *rack* de IA poderá atingir até **65 kW** de densidade térmica. O sistema RDHx será utilizado para remover a maior parte da carga térmica diretamente na fonte de geração de calor, na traseira do *rack*, estimando-se remoção da ordem de **50 kW por *rack***. A carga térmica remanescente, da ordem de aproximadamente **15 kW por *rack***, será tratada pelo sistema *In-Row*, instalado entre os *racks* ou nas extremidades do corredor técnico.

13.5.3. Essa composição é especialmente adequada porque evita depender exclusivamente de ar-condicionado de precisão tradicional para toda a carga térmica dos *racks* de IA. Em um POD com 12 *racks* de 65 kW, a carga térmica total dos *racks* de TI pode alcançar aproximadamente **780 kW**. Caso o RDHx remova cerca de 50 kW por rack, serão removidos aproximadamente **600 kW** diretamente na fonte, restando cerca de **180 kW** a serem tratados pelo sistema *In-Row*. Essa distribuição reduz a exigência sobre o ar do ambiente, melhora o controle térmico, diminui *hotspots* e torna o sistema mais compatível com a alta densidade prevista.

13.5.4. A escolha também está alinhada com referências técnicas de mercado. A Vertiv registra que os *rear-door heat exchangers* complementam a capacidade de resfriamento a ar e que unidades ativas podem alcançar capacidade nominal de até 50 kW, com testes em patamares superiores.

13.5.5. Em comparação com uma solução baseada apenas em *In-Row*, a combinação com RDHx é superior porque remove parcela relevante do calor na fonte, reduzindo a quantidade de ar quente lançada no ambiente e permitindo maior densidade por *rack*. Em comparação com uma solução imediatamente 100% *liquid cooling*, a solução híbrida é mais flexível e menos arriscada, pois não força a Administração a definir, no presente momento, uma arquitetura integralmente líquida antes de conhecer com precisão a composição futura dos servidores de IA disponíveis no mercado.

13.5.6. Assim, a adoção de RDHx + *In-Row* permite atender à demanda atual com resfriamento a ar assistido por água gelada e, ao mesmo tempo, preparar o ambiente para migração gradual para *liquid cooling*, preservando flexibilidade tecnológica e evitando aprisionamento prematuro em uma única arquitetura.

13.6. Arquitetura preparada para migração futura para *liquid cooling*:

13.6.1. A quinta decisão relevante é a preparação do POD para uma futura composição híbrida ou parcial com ***liquid cooling***.

13.6.2. A construção deve atender aos requisitos atuais de resfriamento a ar, mas já contemplar passagens, reforços e infraestrutura necessária para futura implementação de *liquid cooling*. Também prevê que, caso algum *rack* seja substituído por *rack* com resfriamento líquido, as alterações na infraestrutura deverão ser mínimas, aproveitando a tubulação e a lógica hidráulica já concebidas para os RDHx e para os *chillers indoor* com CDU.

13.6.3. Essa escolha é tecnicamente estratégica porque o mercado de servidores de IA ainda está em evolução. Alguns equipamentos de alta densidade são compatíveis com resfriamento a ar assistido, enquanto outros já demandam ou recomendam *liquid cooling*, especialmente em configurações com GPUs de maior potência. Assim, definir desde já uma infraestrutura que permita transição gradual reduz o risco de obsolescência precoce da contratação.

13.6.4. A CDU - *Coolant Distribution Unit* - é um componente importante nessa arquitetura, pois permite isolar o equipamento de TI do circuito de água gelada ou do circuito de fluido da instalação, criando uma rede secundária de fluido com controle de vazão, temperatura e qualidade do fluido. A Vertiv descreve suas unidades XDU como adequadas para aplicações de *direct-to-chip* e *rear door cooling*, inclusive com modelos que operam com ou sem acesso a água gelada do *site*, o que demonstra a importância desse tipo de componente para ambientes de alta densidade.

13.6.5. Portanto, a escolha por uma solução inicialmente *air cooling*, mas preparada para *liquid cooling*, é a mais adequada ao interesse público porque combina viabilidade imediata, menor risco de implantação, compatibilidade com a oferta atual de equipamentos e capacidade de evolução futura. A Administração não ficará limitada a uma arquitetura exclusivamente a ar nem será obrigada a implantar desde o início uma solução integralmente líquida, que poderia gerar custo, complexidade e risco operacional superiores ao necessário no momento inicial.

13.7. *Chillers indoor* com condensação externa:

13.7.1. Em relação às máquinas de resfriamento, optou-se pela adoção de ***chillers* do tipo *indoor***, com condensação externa instalada na laje técnica.

13.7.2. Essa escolha decorre de fatores estruturais, operacionais e de manutenção. A laje técnica possui limitação de carga, estimada em **150 kg/m²**, o que torna recomendável reduzir ao máximo o peso dos equipamentos instalados sobre ela. Ao se adotar *chillers indoor*, desloca-se a maior parte dos componentes de maior massa e complexidade para ambiente interno controlado, mantendo na laje apenas os elementos externos de condensação compatíveis com a capacidade estrutural disponível.

13.7.3. A instalação dos *Chillers* em outro local, como o canteiro ao lado do *data center* ocasionaria uma exposição e riscos a segurança física dos equipamentos, podendo estar sujeitos a vandalismos devido a proximidade com a via pública.

13.7.4. Em comparação com *chillers outdoor* completos, a solução *indoor* reduz o peso concentrado sobre a laje, diminui riscos estruturais, facilita o acesso para manutenção e protege equipamentos sensíveis contra exposição direta a intempéries, poeira, radiação solar e variações ambientais. Também permite melhor integração com a CDU e com os circuitos do POD de IA, simplificando a futura migração de *racks* com RDHx para *racks* com *liquid cooling*.

13.7.5. Além disso, a escolha por *chillers indoor* com CDU integrada ou acoplável favorece a arquitetura híbrida, pois permite que a mesma filosofia de distribuição hidráulica utilizada para os RDHx seja adaptada para alimentação de circuitos de resfriamento líquido. Dessa forma, quando houver substituição de *racks air cooling* por *racks liquid cooling*, a intervenção tende a se concentrar na conexão hidráulica, no *manifold*, na CDU e nos acessórios de distribuição, sem exigir reconstrução ampla da infraestrutura de climatização.

13.7.6. A solução, portanto, é superior à alternativa de instalação de grandes equipamentos *outdoor* na laje, pois reduz o risco estrutural, melhora a manutenibilidade, facilita a integração com o POD e preserva a capacidade de evolução tecnológica.

13.8. Não adoção de central de água gelada tradicional:

13.8.1. Outra questão importante da Solução 1 é a não adoção de uma central de água gelada convencional de grande porte, com tanques de termoacumulação, rede hidráulica extensa, grande quantidade de válvulas, bombas, derivações e pontos de falha.

13.8.2. Embora centrais de água gelada sejam amplamente utilizadas em *data centers*, sua adoção no contexto específico do DC RF poderia aumentar a complexidade de implantação, operação e manutenção. O ambiente do CITEx apresenta histórico de dificuldades relacionadas à disponibilidade e ao manejo de água, o que torna recomendável adotar solução mais simplificada, modular e controlável. Além disso, uma central de água gelada tradicional demandaria maior quantidade de componentes hidráulicos, válvulas, conexões, sensores, bombas e rotas de tubulação, ampliando a probabilidade de falhas, vazamentos, indisponibilidades e necessidade de manutenção especializada.

13.8.3. A solução escolhida simplifica essa arquitetura ao utilizar *chillers indoor* dedicados ao POD de IA, com circuitos mais controlados e integrados aos RDHx, *In-Row* e CDUs. Em vez de utilizar tanque de termoacumulação como *buffer* térmico para o período entre a queda de energia e a entrada dos geradores, a solução adotará UPS dedicada para climatização, garantindo energia temporária aos equipamentos críticos de resfriamento.

13.8.4. Essa abordagem é mais coerente com o objetivo de simplificar a operação, reduzir pontos de falha, diminuir manutenção hidráulica, evitar dependência excessiva de reservatórios de água gelada e assegurar resposta imediata da climatização durante o intervalo de partida e estabilização dos geradores.

13.8.5. Portanto, a não adoção de central de água gelada tradicional decorre de uma decisão técnica voltada à redução de complexidade, menor manutenção, menor risco operacional e maior compatibilidade com um POD de IA de alta densidade em ambiente já existente.

13.9. UPS dedicado para climatização e *continuous cooling*:

13.9.1. Foi considerada a adoção de UPS dedicado à climatização, com capacidade estimada de **350 kW**, para garantir o resfriamento contínuo do POD de IA até a entrada dos geradores.

13.9.2. Essa escolha é crítica porque, em um ambiente de IA com *racks* de até 65 kW, a inércia térmica é muito menor do que em *data centers* convencionais. A interrupção da climatização por poucos minutos pode provocar elevação rápida de temperatura, *hotspots* e desligamento de equipamentos. Assim, não basta manter apenas a carga de TI alimentada por UPS, é necessário manter também a climatização crítica durante o intervalo de transferência para geração por GMG.

13.9.3. A alternativa tradicional seria utilizar tanque de termoacumulação para garantir água gelada durante a transição. Contudo, essa solução exigiria reservatórios, bombas, válvulas, controles adicionais, maior volume de água, mais espaço físico, maior manutenção e maior complexidade hidráulica. No contexto do DC RF, a opção por UPS de climatização é mais simples, direta e compatível com a arquitetura modular proposta.

13.9.4. A própria *Uptime Institute* registra que o Tier IV exige *continuous cooling*, enquanto o Tier III está centrado na manutenção concorrente dos componentes e caminhos de distribuição. Ainda que o objetivo do projeto seja Tier III, a adoção de *continuous cooling* para o POD de IA aumenta a robustez do ambiente e reduz risco térmico durante transições elétricas, o que é especialmente importante em cargas de alta densidade.

13.9.5. Assim, a UPS dedicada à climatização foi escolhida por oferecer resposta imediata, menor complexidade que termoacumulação, maior controle operacional e melhor proteção térmica para o POD de IA durante eventos de transferência, partida e estabilização dos geradores.

13.10. *Chillers* com tecnologia *free cooling*:

13.10.1. A refrigeração representa parcela relevante do consumo energético de um *data center*, especialmente em ambientes de alta densidade. A tecnologia de *free cooling* permite aproveitar condições ambientais favoráveis para reduzir ou dispensar o uso de compressão mecânica em determinados períodos, diminuindo consumo energético e aumentando a eficiência operacional. A *Energy Star* registra que economizadores de ar ou de água podem economizar grande quantidade de energia justamente porque permitem resfriar o *data center* sem operar ar-condicionado ou *chiller* mecânico em determinadas condições, sendo esse princípio usualmente denominado "*free cooling*".

13.10.2. No caso do DC RF, a adoção de *free cooling* é compatível com o objetivo de reduzir OPEX, melhorar eficiência energética e diminuir o esforço dos compressores quando as condições climáticas permitirem. Trata-se de característica especialmente relevante porque o POD de IA terá carga térmica elevada e operação contínua, de modo que pequenas melhorias de eficiência podem gerar impacto expressivo no custo operacional ao longo do ciclo de vida da solução.

13.10.3. Em comparação com chillers convencionais sem *free cooling*, a solução escolhida tende a oferecer melhor eficiência energética, menor desgaste de componentes mecânicos e maior racionalidade operacional. A exigência também se harmoniza com a necessidade de implantar infraestrutura moderna, preparada para IA e com menor custo energético ao longo do tempo.

13.11. Distribuição elétrica flexível por barramento blindado:

13.11.1. Em relação a alimentação dos *racks*, a escolha foi por meio de **barramento blindado aéreo - *busway***.

13.11.2. Essa escolha é coerente com o caráter modular e evolutivo do POD de IA. Em ambientes de alta densidade, a demanda elétrica por *rack* pode variar significativamente conforme a configuração dos servidores, GPUs, *switches*, *storages* e sistemas auxiliares. O *busway* permite maior flexibilidade para adicionar, remover ou reposicionar derivações elétricas, facilitando reconfigurações futuras sem necessidade de grandes intervenções em cabos sob piso.

13.11.3. A alimentação dos *racks* por barramento blindado aéreo, justifica por conferir flexibilidade e escalabilidade à solução, comportando as altas correntes que serão demandadas pelos *racks*.

13.11.4. Em comparação com distribuição elétrica convencional baseada exclusivamente em cabos fixos, o *busway* é mais adequado para ambientes de IA porque facilita alterações de *layout*, expansão de carga, substituição de *racks*, balanceamento de circuitos e manutenção. Essa solução também reduz interferências com o cabeamento lógico sob piso, que será dimensionado para a alta densidade de conexões exigida por *clusters* de computação de alto desempenho.

13.12. Síntese comparativa da Solução 1 em relação às alternativas:

13.12.1. A Solução 1 foi escolhida porque apresenta o melhor equilíbrio entre segurança, disponibilidade, viabilidade estrutural, eficiência energética, manutenibilidade, escalabilidade e aderência à missão institucional.

13.12.2. Em relação ao *container*, a Sala Segura interna é mais permanente, mais integrada, menos exposta fisicamente e mais adequada ao controle institucional do ambiente crítico.

13.12.3. Em relação ao *colocation*, a Solução 1 preserva o controle físico e operacional do Exército, evita dependência de terceiros, reduz exposição indireta da arquitetura tecnológica e cria capacidade própria permanente.

13.12.4. Em relação à nuvem, a Solução 1 evita dependência de provedor externo, assegura soberania de dados, permite operação restrita, melhora previsibilidade orçamentária e atende melhor a cargas de IA sensíveis e estratégicas.

13.12.5. Em relação à alternativa de **geração 2N com geradores de 1,5 MVA**, a solução com 4 (quatro) geradores de 1 MVA em regime 3 + 1 reduz risco estrutural, aproveita os *slots* existentes, diminui custo,

simplifica implantação e permanece aderente à certificação Tier III quando integrada ao projeto elétrico de forma adequada.

13.12.6. Em relação a uma solução de **resfriamento apenas por *In-Row***, a combinação RDHx + *In-Row* é mais adequada para racks de 65 kW, pois remove grande parte do calor diretamente na fonte.

13.12.7. Em relação a uma solução **100% *liquid cooling* desde o início**, a solução híbrida é mais prudente, pois atende ao cenário atual e permite migração gradual com alterações mínimas conforme a evolução dos servidores de IA.

13.12.8. Em relação a uma **central de água gelada tradicional**, a solução com *chillers indoor*, CDU e UPS de climatização reduz complexidade hidráulica, evita tanque de termoacumulação, diminui pontos de falha e simplifica a manutenção.

13.13. Diante dos aspectos analisados, conclui-se que a Solução 1 - **expansão da Sala Segura Modular dentro do DC RF** - é a alternativa mais adequada ao interesse público, pois aproveita infraestrutura existente, fortalece a capacidade própria do Exército Brasileiro, preserva a soberania sobre dados e ativos críticos, possibilita certificação Tier III, suporta cargas de IA de alta densidade e permite evolução tecnológica gradual para liquid cooling.

13.14. A solução de geração com 4 (quatro) geradores de 1 MVA em configuração N+1, a adoção de POD de IA com 12 (doze) racks de alta densidade, a combinação RDHx + *In-Row,* o emprego de *chillers indoor* com CDU e *free cooling*, a UPS dedicada à climatização e a não adoção de central de água gelada tradicional compõem uma arquitetura coerente, eficiente e tecnicamente justificada.

13.15. Portanto, a Solução 1 não apenas resolve a necessidade imediata de expansão do DC RF, mas também prepara o Data Center Coronel Ricardo Franco para atuar como infraestrutura estratégica de processamento de IA do Exército Brasileiro, com segurança, disponibilidade, escalabilidade e autonomia operacional.

14. Estimativa de custo total da contratação

Valor (R$): 63.400.000,00

14.1. A estimativa do valor da contratação foi elaborada com base em pesquisa preliminar de mercado, utilizando composição de preços por macrocomponentes da solução de expansão do Data Center Corporativo do Exército Brasileiro, que contempla nova Sala Segura, certificação Uptime, infraestrutura elétrica, UPS, baterias, grupos moto geradores, climatização, racks, cabeamento estruturado, segurança, monitoramento, combate a incêndio, moving, implantação de POD de IA, implantação de PODs padrão e demais subsistemas necessários à ampliação do ambiente crítico.

14.2. A composição do valor estimado observa, em nível de Estudo Técnico Preliminar, a necessidade de compatibilidade com os valores praticados pelo mercado e com o art. 23 da Lei nº 14.133/2021, devendo ser posteriormente consolidada na fase de Termo de Referência mediante pesquisa formal de preços, análise crítica das propostas, saneamento de escopo e verificação dos quantitativos definitivos.

14.3. Para fins de planejamento, a estimativa foi estruturada a partir dos itens aderentes ao escopo principal da solução escolhida, qual seja, a **expansão interna da Sala Segura Modular do *Data Center* Coronel Ricardo Franco**, com capacidade para suportar ambiente de alta densidade destinado ao processamento de Inteligência Artificial e, adicionalmente, a implantação de **2 (dois) PODs padrão**, voltados à hospedagem de cargas convencionais de TIC, de menor densidade energética e térmica.

14.4. A inclusão dos **2 (dois) PODs padrão** justifica-se pela necessidade de melhor aproveitamento da infraestrutura expandida e pela possibilidade de absorção de demandas futuras de hospedagem de servidores e ativos de TIC que não exijam a mesma densidade do POD de IA. Para fins de estimativa, considerou-se acréscimo de **R$ 2.800.000,00 por POD padrão**, contemplando a infraestrutura associada, máquinas de climatização adicionais, *nobreaks*/ UPS complementares, adequações elétricas, *racks*, cabeamento e demais componentes necessários à sua operação integrada ao ambiente do *data center*.

14.5. A composição estimada considera os seguintes macrocomponentes (os quais serão convertidos/ adaptados em itens do processo de contratação):

Item	Macrocomponente da solução	Valor estimado
1	Expansão de capacidade, Sala Segura, passagens seladas, piso, forro, quadros, PDUs, aterramento e certificação *Uptime*	R$ 13.613.425,06
2	Sistema ininterrupto de energia - UPS para carga crítica de IA, UPS para climatização, baterias de lítio e infraestrutura associada	R$ 12.482.788,77
3	Sistema ininterrupto de energia - UPS para carga crítica de TI dos dois POD padrão de servidores	R$ 2.901.897,05
4	Grupos moto geradores, chave de transferência automática, disjuntores de interligação e sistema de tanque para reabastecimento	R$ 6.235.941,60
5	Sistema de climatização de precisão com *chiller indoor* para atender sistema *Rear Door* para atendimento ao POD de IA	R$ 9.948.608,00
6	Sistema de climatização de precisão com máquinas *In-Row* para atender a carga térmica mínima de 300 kW do POD de IA	R$ 4.134.208,00
7	Sistema de climatização de precisão com máquinas In-Row condensadora para atender a carga de TI do POD Padrão de servidores (165 kW).	R$ 2.800.592,00
8	Transformadores de Potência e interligação elétrica de média para baixa tensão	R$ 1.050.020,00
9	*Racks* com *Rear Door* para alta densidade térmica	R$ 3.216.423,17
10	*Racks* preparados para evolução futura com resfriamento *liquid cooling*	R$ 907.408,00
11	Racks padrão de servidor montados em 2 POD de 12 und cada	R$ 115.172,80
12	Cabeamento estruturado entre *racks* de telecomunicações	R$ 395.789,00
13	Cabeamento estruturado entre *racks* de telecomunicações e *racks* de IA	R$ 1.578.528,00
14	Cabeamento estruturado entre *racks* de telecomunicações e *racks* do POD Padrão	R$ 1.420.458,00
15	Sistema e software de segurança e monitoramento	R$ 2.273.536,00
16	Serviços de movimentação - *moving* - de ativos de TIC	R$ 298.960,00
	Valor global estimado da contratação	**R$ 63.373.755,45**

14.6. Para fins de planejamento orçamentário, considerando os arredondamentos próprios da fase preliminar e a necessidade de compatibilização posterior dos quantitativos no Termo de Referência, adota-se como **valor estimado de referência da contratação o montante de R$ 63.400.000,00**.

14.7. O valor estimado é compatível com a complexidade técnica do objeto, pois contempla não apenas a implantação do ambiente de IA de alta densidade, mas também a expansão da capacidade geral do *data center* por meio de 2 (dois) PODs padrão, permitindo maior aproveitamento da infraestrutura instalada, melhor organização física dos ativos de TIC e ampliação da capacidade de hospedagem de cargas computacionais convencionais.

14.8. A estimativa contempla os macrocomponentes essenciais para a implantação da solução escolhida, abrangendo infraestrutura física, energia crítica, climatização especializada, *racks* de alta densidade, *racks* e infraestrutura para PODs padrão, conectividade passiva, monitoramento, segurança, combate a incêndio, *moving* e certificação. A composição deverá ser refinada na etapa de Termo de Referência, com detalhamento dos quantitativos, consolidação de memoriais técnicos, análise crítica dos preços e validação da compatibilidade entre o escopo técnico e o orçamento estimado.

14.9. A adoção do valor estimado de **R$ 63.400.000,00** mostra-se adequada para fins de planejamento da contratação, pois decorre de pesquisa de mercado específica para solução de *data center*, está vinculada aos componentes essenciais da expansão pretendida e reflete o custo esperado para implantação de ambiente próprio, seguro, redundante, preparado para processamento de Inteligência Artificial e apto a absorver demandas adicionais de TIC por meio dos PODs padrão.

14.10. Conclui-se, portanto, que a contratação possui valor estimado de referência de **R$ 63.400.000,00**, devendo esse montante subsidiar o planejamento orçamentário, a análise de viabilidade econômica e a elaboração do Termo de Referência, sem prejuízo de refinamento posterior a partir da pesquisa formal de preços, do Projeto Executivo e da consolidação definitiva dos quantitativos.

14.11. Ressalta-se que o valor de **R$ 63.400.000,00** utilizado neste Estudo Técnico Preliminar corresponde à estimativa preliminar obtida durante a fase de levantamento e comparação das soluções, a partir das cotações disponíveis naquele momento, tendo sido utilizado para subsidiar a análise de viabilidade técnica e econômica da contratação.

14.12. Posteriormente, durante a elaboração do Termo de Referência e a realização da pesquisa formal de preços, houve o refinamento dos valores dos componentes da solução com base nas propostas e referências de preços efetivamente obtidas para as especificações e quantitativos consolidados, resultando no valor estimado final da contratação de **R$ 59.587.298,11 (cinquenta e nove milhões, quinhentos e oitenta e sete mil, duzentos e noventa e oito reais e onze centavos).**

14.13. Dessa forma, para fins da licitação e da definição do valor estimado da contratação, prevalece o valor de R$ 59.587.298,11, constante do Termo de Referência, permanecendo os valores anteriormente indicados neste ETP como registros da estimativa preliminar utilizada na análise comparativa das alternativas.

14.14. A formação dos preços estimados da contratação foi realizada mediante pesquisa formal de preços, utilizando fontes compatíveis com os parâmetros previstos na regulamentação aplicável, especialmente consultas ao Portal de Compras Governamentais e consulta direta a fornecedores especializados no fornecimento e implantação de infraestrutura crítica de Data Center.

14.15. As referências obtidas no Portal de Compras Governamentais foram analisadas quanto à similaridade e à efetiva comparabilidade com os componentes da solução pretendida. Considerando o elevado grau de especificidade do objeto, caracterizado pela integração entre Sala Segura, energia crítica, climatização de alta densidade, racks, cabeamento, sistemas de segurança e monitoramento, moving e certificação Tier III, determinadas contratações públicas pesquisadas não apresentaram equivalência técnica suficiente para utilização direta na composição dos preços, sendo utilizadas como referências auxiliares para avaliação da compatibilidade dos valores praticados no mercado.

14.16. Para os componentes cuja especificidade técnica limitou a obtenção de referências públicas plenamente comparáveis, foram consideradas consultas diretas a fornecedores especializados, realizadas a partir de especificações técnicas uniformes e correspondentes ao objeto pretendido, de forma a assegurar comparabilidade entre as propostas recebidas quanto ao escopo, quantitativos, capacidades, instalação, integração, garantia e demais obrigações associadas à solução.

14.17. Os valores unitários adotados no Termo de Referência resultaram da análise crítica das referências e propostas obtidas na pesquisa formal de preços, considerando sua aderência às especificações técnicas, aos quantitativos e às condições de fornecimento estabelecidas para a contratação. As referências sem compatibilidade técnica suficiente foram desconsideradas da formação direta do preço, permanecendo nos autos como elementos auxiliares de pesquisa. A documentação comprobatória das fontes consultadas, propostas recebidas e respectivos valores integra o processo administrativo da contratação.

15. Justificativa técnica da escolha da solução

15.1. A escolha da **Solução 1 - Expansão da Sala Segura Modular dentro do *Data Center* Coronel Ricardo Franco** justifica-se tecnicamente por ser a alternativa que melhor atende aos requisitos de processamento de Inteligência Artificial, segurança, disponibilidade, escalabilidade, continuidade operacional, controle institucional, integração com a infraestrutura existente e evolução tecnológica do ambiente de *data center* do Exército Brasileiro.

15.2. A solução escolhida consiste na implantação de uma nova Sala Segura Modular em área técnica já existente no interior do próprio edifício do *Data Center* Coronel Ricardo Franco - DC RF, aproveitando espaço previamente concebido para expansão e atualmente disponível. Essa característica permite reduzir intervenções externas, preservar o perímetro de segurança já estabelecido, facilitar a integração com os sistemas existentes e consolidar a capacidade de processamento de IA em ambiente próprio e controlado pela Administração.

15.3. Do ponto de vista técnico, a solução é aderente à necessidade central da contratação, que é preparar o DC RF para hospedar Soluções de Infraestrutura de IA - SIIA, compostas por servidores acelerados por GPU, *storages* de alto desempenho, redes de alta velocidade, sistemas de energia crítica, climatização de precisão, monitoramento, segurança física e demais componentes necessários à operação de cargas computacionais intensivas.

15.4. A infraestrutura proposta é compatível com o dimensionamento previsto neste ETP, especialmente quanto à implantação de ambiente de alta densidade composto por 12 *racks* de processamento de IA, com capacidade individual de até 65 kVA, totalizando carga crítica de TI de aproximadamente 780 kVA e capacidade de planejamento de até 800 kVA. Esse dimensionamento é tecnicamente adequado à natureza das cargas de IA, que concentram elevada demanda elétrica e térmica em poucos *racks*, diferentemente de ambientes corporativos convencionais.

15.5. A adoção de *racks* de alta densidade justifica-se pela evolução dos *workloads* de Inteligência Artificial, especialmente treinamento, ajuste fino, inferência, modelos de linguagem de grande porte, análise massiva de dados, visão computacional, automação, busca semântica e aplicações generativas. Tais cargas demandam servidores com múltiplas GPUs, alta largura de banda, elevada capacidade de memória, armazenamento de alto desempenho e redes de interconexão de baixa latência, requisitos que não podem ser adequadamente suportados por infraestrutura tradicional de *data center*.

15.6. A solução interna em Sala Segura mostra-se tecnicamente superior às alternativas externas ou terceirizadas, pois permite que os ativos críticos, os dados, os modelos, os fluxos de processamento, os *logs*, os artefatos de IA e os mecanismos de operação permaneçam sob controle físico, lógico e administrativo do Exército Brasileiro. Essa condição é essencial para preservar soberania, segurança da informação, rastreabilidade, cadeia de custódia e continuidade dos serviços estratégicos.

15.7. A escolha também se justifica pela compatibilidade com o ambiente atual do DC RF, que já possui infraestrutura de missão crítica, operação especializada, governança estabelecida, conectividade corporativa, mecanismos de segurança, rotinas de monitoramento e certificação Tier III em *Design* e *Facilities*. A expansão interna permite que a nova capacidade de IA seja incorporada ao ecossistema existente, reduzindo riscos de integração e evitando a criação de ilhas operacionais desconectadas da arquitetura atual.

15.8. Sob o aspecto de disponibilidade, a solução escolhida preserva os requisitos de ambiente crítico, especialmente quanto à redundância, manutenibilidade concorrente e continuidade operacional. A expansão deverá ser concebida, executada, comissionada e documentada de forma compatível com os critérios de certificação Tier III, evitando descaracterização da topologia certificada e assegurando que intervenções planejadas possam ocorrer sem interrupção da operação de TI.

15.9. A exigência de Projeto Executivo detalhado é tecnicamente indispensável, pois a solução envolve integração de múltiplos subsistemas críticos: civil, estrutural, elétrica, sala segura, climatização, combate a incêndio, rede passiva, monitoramento, segurança física, CFTV, *moving*, documentação, recuperação das áreas afetadas e paisagismo. A complexidade da solução exige compatibilização prévia entre disciplinas, evitando conflitos de projeto, subdimensionamentos, interferências físicas, riscos operacionais e custos adicionais durante a execução.

15.10. A solução de energia elétrica é tecnicamente justificada pela necessidade de suportar cargas críticas de alta densidade com fornecimento contínuo, estável e seguro. Para isso, a arquitetura deverá contemplar subestação, grupos moto geradores, UPS modulares do tipo *True On-Line*, quadros elétricos, PDUs de alta capacidade,

cabeamento elétrico, SPDA, aterramento e demais componentes necessários à operação segura de equipamentos sensíveis e de alto consumo.

15.11. A adoção de solução de geração com 4 (quatro) grupos geradores de 1 MVA, em configuração 3 + 1, mostra-se tecnicamente adequada por aproveitar a concepção e os espaços existentes, reduzir riscos estruturais associados a equipamentos de maior porte, simplificar a implantação, preservar a escalabilidade e manter aderência à lógica de redundância necessária a ambiente de missão crítica. Essa arquitetura permite sustentar a carga projetada, com reserva operacional, sem impor complexidade excessiva à infraestrutura civil e elétrica.

15.12. A previsão de autonomia mínima de combustível compatível com os requisitos de disponibilidade, bem como a análise de ampliação dos tanques existentes, justifica-se pela criticidade do ambiente de IA. Cargas computacionais intensivas não admitem interrupções abruptas sem risco de perda de processamento, degradação de serviços, indisponibilidade de aplicações e impacto sobre sistemas corporativos e estratégicos hospedados ou integrados ao DC RF.

15.13. A solução de climatização adotada é tecnicamente adequada ao cenário de IA de alta densidade, pois combina resfriamento a ar otimizado, confinamento térmico, máquinas *In-Row*, trocadores de calor do tipo *Rear Door Heat Exchanger* - RDHx, *chillers indoor* com condensação externa, CDU e preparação para futura evolução para *liquid cooling*. Essa arquitetura híbrida permite remover grande parte do calor próximo à fonte de geração, reduzir a sobrecarga do ambiente, melhorar a eficiência térmica e preservar a operação segura dos equipamentos.

15.14. A combinação RDHx + *In-Row* é tecnicamente mais adequada do que uma solução baseada apenas em climatização convencional, pois *racks* de até 65 kVA concentram carga térmica incompatível com a lógica tradicional de resfriamento perimetral. O uso de *rear door* permite capturar o calor na saída dos servidores, enquanto os equipamentos *In-Row* contribuem para o controle térmico do corredor confinado, melhorando a estabilidade ambiental e reduzindo o risco de pontos quentes.

15.15. A opção por arquitetura inicialmente baseada em *air cooling* assistido, mas preparada para *liquid cooling*, é tecnicamente prudente. O mercado de servidores de IA encontra-se em rápida evolução, havendo equipamentos que ainda operam com resfriamento a ar de alta performance e outros que já demandam resfriamento líquido direto. Assim, a solução evita tanto o subdimensionamento de uma infraestrutura exclusivamente a ar quanto a adoção prematura de uma arquitetura 100% líquida, mais complexa e onerosa.

15.16. A previsão de infraestrutura *liquid cooling ready*, com espaços, rotas, tubulações, coletores, válvulas, engates rápidos e possibilidade futura de CDUs, reduz o risco de obsolescência precoce da contratação. Essa decisão permite que, no futuro, a Administração substitua ou acrescente *racks* com resfriamento líquido com menor intervenção física, preservando a continuidade operacional e prolongando a vida útil da infraestrutura implantada.

15.17. A não adoção de uma central de água gelada tradicional de grande porte também possui justificativa técnica no contexto específico do Data Center Coronel Ricardo Franco. Embora esse tipo de solução seja usual em determinadas arquiteturas de data center, sua implantação, neste caso, poderia ampliar a complexidade hidráulica, a quantidade de bombas, válvulas, sensores, derivações, trechos de tubulação, pontos potenciais de falha, necessidades de manutenção especializada e riscos associados a vazamentos em áreas críticas.

15.18. A adoção de chillers indoor, com condensadoras externas/remotas e infraestrutura preparada para CDU, quando prevista no Projeto Executivo, mostra-se mais aderente às limitações físicas, estruturais e operacionais do edifício existente. Essa arquitetura permite concentrar os principais componentes elétricos, hidráulicos e de controle em ambiente técnico interno, protegido e acessível, reduzindo a exposição de equipamentos críticos à radiação solar, chuva, poeira, umidade, intempéries e demais condições ambientais adversas que podem acelerar a degradação de componentes e reduzir a confiabilidade ao longo do ciclo de vida da solução.

15.19. Sob o aspecto estrutural, a solução com chillers indoor reduz a necessidade de instalação de grandes equipamentos de produção de água gelada em coberturas, lajes ou áreas externas que não tenham sido originalmente concebidas para tais cargas. Dessa forma, preserva-se a integridade da edificação existente, minimizam-se intervenções civis de maior porte e evita-se a imposição de esforços estruturais adicionais incompatíveis com a premissa de aproveitamento das áreas técnicas já disponíveis no Data Center.

15.20. Do ponto de vista operacional, a proximidade entre a produção e o controle do fluido de resfriamento e as cargas críticas de TI favorece a redução do comprimento dos circuitos hidráulicos, melhora a resposta do sistema às

variações de carga térmica e permite controle mais rigoroso da temperatura de saída da água gelada e/ou do fluido técnico de resfriamento, inclusive solução de água com propilenoglicol a 25% — PG25, quando especificada no Projeto Executivo. Essa característica é relevante para ambientes de alta densidade, nos quais pequenas variações térmicas podem impactar a eficiência, a estabilidade e a vida útil dos servidores acelerados por GPU.

15.21. A arquitetura proposta também favorece a coexistência entre resfriamento a ar de alta capacidade e futura evolução para resfriamento líquido, sem impor, desde a fase inicial, a adoção integral de liquid cooling. A previsão de rotas, tubulações, coletores, válvulas, engates rápidos e CDU, quando aplicável, permite que a Administração evolua gradualmente para arquiteturas direct-to-chip ou equivalentes, conforme a evolução dos servidores de IA e a real necessidade de dissipação térmica, reduzindo risco de obsolescência precoce e evitando futuras obras civis invasivas.

15.22. A manutenção dos principais componentes em ambiente interno e protegido também aumenta a disponibilidade operacional do sistema, pois permite inspeções, manutenções preventivas, corretivas e ajustes de parâmetros independentemente de horário, chuva, incidência solar, poeira ou outras condições climáticas externas. Essa característica facilita o acompanhamento pela equipe técnica da Administração, reduz riscos durante intervenções e é compatível com ambientes de missão crítica que exigem elevados índices de disponibilidade.

15.23. A solução também se integra de forma mais eficiente ao gerenciamento térmico do Data Center por meio de DCIM, IHMs locais, sensores ambientais e sistemas de supervisão. A instalação dos principais pontos de leitura, controle e operação em áreas técnicas protegidas facilita a visualização de alarmes, o ajuste de parâmetros, o acompanhamento em tempo real das condições de operação e a rápida resposta a eventos anormais, contribuindo para maior segurança operacional.

15.24. Dessa forma, a adoção de chillers indoor com condensadoras externas/remotas, associada à infraestrutura preparada para CDU e à UPS dedicada à climatização, constitui solução tecnicamente justificada para o contexto do DC RF, pois reduz complexidade hidráulica, evita central de água gelada tradicional de grande porte, melhora a manutenibilidade, favorece o controle térmico próximo à carga crítica, reduz exposição de componentes sensíveis e preserva a flexibilidade de evolução tecnológica para liquid cooling.

15.25. A adoção de UPS dedicada à climatização, para assegurar *continuous cooling*, é tecnicamente justificada porque equipamentos de IA de alta densidade possuem baixa tolerância à elevação térmica. Durante o intervalo entre a queda da energia comercial e a entrada estabilizada dos geradores, a manutenção da climatização é essencial para evitar desligamentos, degradação de desempenho, acionamento de proteções térmicas e riscos aos ativos de alto valor.

15.26. A Sala Segura Modular é tecnicamente necessária para prover proteção física compatível com a criticidade dos ativos de IA. Sua estrutura deve assegurar resistência ao fogo, estanqueidade, proteção contra água, pó, fumaça, acesso indevido e demais riscos ambientais, além de integração com os sistemas de detecção e combate a incêndio, controle de acesso, CFTV, monitoramento ambiental e resposta a incidentes.

15.27. A solução de combate a incêndio com detecção precoce, HSSD, agente limpo, lógica cruzada de disparo, estações de abortamento, acionamento manual e integração ao monitoramento é tecnicamente adequada a ambiente de TIC, pois reduz o risco de dano aos equipamentos, permite identificação antecipada de eventos e preserva a segurança dos ativos sem uso de agentes incompatíveis com equipamentos eletrônicos sensíveis.

15.28. A infraestrutura física dos *racks* e do piso também justifica tecnicamente a solução escolhida. *Racks* de IA podem concentrar elevado peso em pequena área, especialmente quando equipados com servidores acelerados por GPU, *switches*, PDUs, cabeamento de alta performance e demais componentes. Por essa razão, a solução deve contemplar *racks* de alta capacidade estrutural, piso compatível com cargas elevadas, organização em fileiras, corredores confinados e *layout* que favoreça manutenção, circulação segura e eficiência térmica.

15.29. A solução de rede passiva é tecnicamente indispensável para o processamento de IA, pois *clusters* de GPU dependem de alta capacidade de comunicação entre servidores, *storages* e ativos de rede. A previsão de *racks* de telecomunicações, DIOs modulares, cabeamento óptico adequado e soluções pré-conectorizadas reduz riscos de perda, falhas de instalação, retrabalho, latência indevida e indisponibilidade durante a implantação ou expansão.

15.30. O monitoramento integrado por DCIM, sensores ambientais, sensores de líquido, medição elétrica, alarmes, notificações, integração com incêndio, visualização em *videowall* e acompanhamento em tempo real é tecnicamente necessário para garantir operação segura de ambiente de alta densidade. Em cargas de IA, pequenas variações de

temperatura, umidade, consumo, fluxo de ar ou alimentação elétrica podem gerar impactos relevantes, razão pela qual a visibilidade operacional deve ser ampliada.

15.31. A adoção de controle de acesso, CFTV, biometria facial, fechaduras eletromagnéticas e recursos analíticos de vídeo é tecnicamente justificada pela criticidade dos ativos hospedados. O ambiente de IA processará dados, modelos e sistemas estratégicos, exigindo controle rigoroso de acesso, rastreabilidade de eventos, prevenção contra intrusão, auditoria e resposta rápida a ocorrências físicas.

15.32. A previsão de moving, documentação *as built*, identificação da infraestrutura, testes, comissionamento, treinamento e suporte técnico também integra a justificativa técnica da solução. A movimentação ou reorganização de ativos críticos deve ocorrer com planejamento, seguro, procedimentos de mitigação de *downtime* e validação pós-implantação, de modo a preservar a continuidade dos serviços e garantir que a equipe técnica receba ambiente documentado e operável.

15.33. A escolha da Solução 1 também se justifica pela possibilidade de expansão futura. Além do POD de IA, o ETP prevê a possibilidade de implantação de novos PODs padrão, destinados a cargas de menor densidade. Essa flexibilidade permite melhor aproveitamento da infraestrutura instalada e prepara o DC RF para demandas futuras, sem necessidade de novas intervenções estruturais de grande porte em curto prazo.

15.34. Em comparação com a solução por container, a Sala Segura interna é tecnicamente mais integrada, mais permanente, menos exposta fisicamente e mais aderente ao controle institucional do ambiente crítico. O *container*, embora modular e potencialmente mais rápido de implantar, exigiria interfaces externas adicionais, maior proteção perimetral, interligações físicas mais complexas e maior exposição a intempéries e riscos externos.

15.35. Em comparação com o *colocation*, a solução interna preserva o controle físico e operacional do Exército Brasileiro, evita dependência de infraestrutura de terceiros, reduz exposição indireta da arquitetura tecnológica e permite que os requisitos de segurança, disponibilidade, monitoramento, acesso e operação sejam definidos e fiscalizados diretamente pela Administração.

15.36. Em comparação com a nuvem, a solução interna assegura maior soberania sobre dados, modelos, fluxos de processamento e ativos críticos, além de permitir operação em ambiente restrito, com governança própria e maior previsibilidade técnica. A nuvem pode ser útil para cargas complementares ou temporárias, mas não substitui a necessidade de infraestrutura própria para cargas estratégicas, sensíveis e de alta criticidade.

15.37. Dessa forma, a Solução 1 apresenta a melhor aderência técnica aos requisitos definidos no ETP, pois combina alta densidade elétrica, climatização especializada, segurança física, disponibilidade, monitoramento, integração ao ambiente existente, preparação para evolução tecnológica, preservação da certificação Tier III e fortalecimento da capacidade própria do Exército Brasileiro.

15.38. Conclui-se que a **Expansão da Sala Segura Modular dentro do *Data Center* Coronel Ricardo Franco** é tecnicamente justificada por atender de forma mais completa, segura e evolutiva à necessidade de implantação de infraestrutura estratégica de processamento de Inteligência Artificial, garantindo ao Exército Brasileiro autonomia operacional, proteção dos ativos críticos, capacidade de crescimento e sustentação de cargas computacionais de alta densidade ao longo do ciclo de vida da solução.

15.39. **Do Parcelamento da Contratação Decorrente de Aspectos Técnicos:**

15.39.1. Considerando que a solução de *data center* compõe-se de itens interdependentes e interoperáveis entre si, e ainda que a falha em um dos subsistemas pode comprometer o funcionamento dos demais, comprometendo a alta disponibilidade e segurança, não verifica-se a possibilidade de parcelamento decorrente de aspectos técnicos.

15.39.2. Nesse mesmo sentido, considerando que a expansão da Sala Segura Modular dentro do *Data Center* Coronel Ricardo Franco constitui-se de múltiplos subsistemas críticos (civil, estrutural, elétrica, sala segura, climatização, combate a incêndio, rede passiva, monitoramento, segurança física, CFTV, *moving*, documentação, recuperação das áreas afetadas e paisagismo), aliado a complexidade da solução, é imperioso a compatibilização prévia entre os itens, evitando conflitos de projeto, subdimensionamentos, interferências físicas, riscos operacionais e custos adicionais durante a execução, fator que afasta tecnicamente a possibilidade de parcelamento e exige a contratação dos diversos itens em grupo único.

15.39.3. A contratação da solução em um grupo único, o qual abrangerá todos os materiais e serviços de todos os ambientes e subsistemas, também visa garantir a padronização da execução dos serviços e a integração com o *data center* já em operação, tendo em vista que o mesmo consiste em uma solução integrada. Destaca-se ainda a necessidade de garantir a interoperabilidade, evitar incompatibilidades ou prejuízos na garantia e suporte técnico, e ainda possibilitar um eficiente gerenciamento da solução a ser contratada e do ambiente tecnológico que será inserida.

15.39.4. Em análise das peculiaridades do mercado de TIC verifica-se que a contratação de solução que abranja a totalidade da expansão do *data center* não compromete a competitividade do certame e não reduz a economia de escala. A contratação dos itens de forma segregada expõe à Administração a riscos da contratação, como no caso da falta de licitantes interessados em fornecer determinado item (ou em caso de inabilitação de propostas e/ou fornecedores), podendo esse restar fracassado, inviabilizando assim a implantação da solução, que é composta por um conjunto de itens.

15.39.5. Em outros termos, justifica-se a adoção da contratação da solução centralizada em um único grupo em razão da viabilidade técnica, pois, garante a padronização das características essenciais entre os componentes da solução, bem como a integração dos mesmos, considerando que essa padronização visa prevenir futuros prejuízos aos cofres públicos e que os itens deverão ser compatíveis e funcionar em conjunto.

15.39.6. A necessidade de contratação da solução em grupo único não se confunde com a obrigação de implementação financeira integral e imediata de todos os componentes. A solução deverá permanecer sob responsabilidade integrada de um único fornecedor ou consórcio contratado, de forma a garantir a compatibilidade entre os subsistemas de energia, climatização, sala segura, racks, cabeamento, monitoramento, segurança, automação e demais componentes, evitando conflitos de projeto, incompatibilidades técnicas, fragmentação de responsabilidades e riscos à certificação e à disponibilidade do Data Center.

15.39.7. A execução física e financeira da solução ocorrerá de forma gradual, em consonância com a sequência técnica de implantação e com a disponibilização dos recursos orçamentários destinados ao projeto. Essa característica torna necessária a adoção de mecanismo que preserve a unicidade técnica da solução e, simultaneamente, permita à Administração adequar a efetiva contratação e o correspondente desembolso à disponibilidade dos recursos ao longo da implantação.

15.39.8. Dessa forma, a utilização do Sistema de Registro de Preços permite compatibilizar dois requisitos da contratação: de um lado, a manutenção de uma solução única e integrada, adjudicada em grupo único, preservando a responsabilidade técnica pela interoperabilidade e funcionamento conjunto dos subsistemas; de outro, a possibilidade de implementação gradual, conforme a liberação de recursos e a evolução das etapas previstas para o empreendimento.

15.39.9. A execução gradual prevista para o empreendimento será operacionalizada mediante contratações sucessivas decorrentes da Ata de Registro de Preços, em função da disponibilidade efetiva dos recursos orçamentários destinados ao projeto. A primeira contratação não implicará, necessariamente, o consumo integral dos quantitativos registrados.

15.39.10. Os contratos subsequentes deverão preservar a concepção integrada da solução e observar as especificações, interfaces, projetos e condicionantes técnicas estabelecidas para o empreendimento, de modo que a implantação gradual não resulte em fragmentação tecnológica ou incompatibilidade entre subsistemas.

15.39.11. A utilização de uma mesma Ata e de um único adjudicatário para o grupo permite conciliar a contratação progressiva dos quantitativos com a manutenção de responsabilidade técnica integrada sobre a solução, reduzindo os riscos de incompatibilidade, conflitos entre fornecedores, perda de garantia e dificuldades na determinação de responsabilidades.

16. Justificativa econômica da escolha da solução

16.1. A escolha da Solução 1 - **Expansão da Sala Segura Modular dentro do Data Center Coronel Ricardo Franco** justifica-se economicamente por apresentar a melhor relação entre custo total, benefício institucional, permanência do ativo, previsibilidade orçamentária, segurança, soberania de dados e capacidade de atendimento à demanda de processamento de Inteligência Artificial ao longo do ciclo de vida da solução.

16.2. A análise econômica não deve se restringir ao menor custo inicial aparente, tendo em vista que a contratação envolve infraestrutura crítica de *data center*, com alta densidade elétrica e térmica, requisitos de continuidade operacional, preservação da certificação Tier III, segurança física, segurança da informação e suporte a cargas estratégicas de IA. Nesse contexto, a vantajosidade deve ser aferida pelo **Custo Total de Propriedade - TCO**, pela formação de capacidade própria e pela redução de dependência de terceiros.

16.3. O estudo consolidou, para a Solução 1, valor de referência de **R$ 63.400.000,00**, contemplando a implantação da Sala Segura Modular interna, do POD de IA e de **2 (dois) PODs padrão**. Considerando a mesma proporção de manutenção preditiva e corretiva utilizada na análise de ciclo de vida, estima-se custo adicional de manutenção da ordem de **R$ 20.800.000,00** no horizonte decenal, resultando em **TCO estimado de aproximadamente R$ 84.200.000,00 em 10 anos**. Considerando a carga de TI adicional de aproximadamente **1.130 kW**, o valor de referência da contratação corresponde a aproximadamente **R$ 56.106,19/kW**, enquanto o TCO decenal estimado corresponde a aproximadamente **R$ 74.512,21/kW**.

16.4. A Solução 2, baseada em *container*, não demonstrou vantagem econômica em relação à expansão interna. Considerando o novo escopo da contratação, que contempla POD de IA e 2 (dois) PODs padrão, a Solução 1 possui valor de referência de **R$ 63.400.000,00**, enquanto a Solução 2, atualizada proporcionalmente para escopo equivalente, alcança valor comparativo mínimo estimado de **R$ 66.650.000,00**. Além disso, a solução em *container* apresenta menor robustez de pesquisa de preços e tende a exigir custos adicionais de implantação externa, fundações, interligações, segurança perimetral, proteção contra intempéries, integração elétrica, lógica, de monitoramento e de combate a incêndio.

16.5. A comparação com referências externas de mercado reforça a razoabilidade econômica da Solução 1. A JLL registra que o custo médio global de construção de *data centers* aumentou de **US$ 7,7 milhões/MW em 2020 para US$ 10,7 milhões/MW em 2025**, com previsão de **US$ 11,3 milhões/MW em 2026**, sem incluir o *fit-out* tecnológico específico para IA. A *Turner & Townsend* também aponta que *data centers* de maior densidade, com resfriamento líquido, podem apresentar prêmio médio de **7% a 10%** em relação a soluções equivalentes refrigeradas a ar, em razão da maior complexidade técnica dos sistemas de climatização e infraestrutura.

16.6. A Solução 3, baseada em *colocation*, embora reduza investimento inicial próprio, transforma a necessidade em despesa recorrente. Como referência de mercado, a CBRE registrou preço médio de **US$ 196,25/kW/mês** para demandas de 250 kW a 500 kW em mercados primários de *wholesale colocation*. Aplicando-se esse valor à carga de planejamento atualizada de **1.130 kW**, com taxa de câmbio referencial de **R$ 5,0071/US$**, o custo estimado alcançaria aproximadamente **R$ 1.110.387,01 por mês**, **R$ 13.324.644,17 por ano** e **R$ 133.246.441,65 em 10 anos** , sem incluir aquisição de *hardware*, *links* dedicados, *cross-connects*, seguros, suporte remoto, migração, custos de saída e requisitos adicionais de segurança.

16.7. Além do custo recorrente elevado, a alternativa de *colocation* possui incerteza técnica relevante para cargas de IA de alta densidade. O *Uptime Institute* registra que mais de **80% dos operadores pesquisados não possuem *racks* acima de 30 kW**, enquanto o ambiente previsto neste ETP demanda suporte a *racks* de até **65 kVA**, indicando que a oferta de ambientes de mercado aptos a esse perfil de carga é restrita.

16.8. A Solução 4, baseada em nuvem, também não se mostra economicamente mais vantajosa como solução principal para operação contínua de cargas estratégicas de IA e hospedagem complementar dos 2 (dois) PODs padrão. O próprio estudo registra estimativa de aproximadamente **R$ 550.000,00 por mês** para o núcleo de IA, o que representa **R$ 66.000.000,00 em 10 anos** apenas em computação. Considerando acréscimo mínimo de referência

para os 2 (dois) PODs padrão, o custo comparativo mínimo alcançaria **R$ 71.600.000,00 em 10 anos**, sem considerar armazenamento, tráfego de saída, suporte, licenciamento, serviços gerenciados, segurança, governança financeira e custos de migração.

16.9. *Benchmarks* públicos de provedores de nuvem indicam que a operação contínua de capacidade equivalente pode superar esse valor. A AWS informa que a instância **p5.48xlarge** possui **8 GPUs NVIDIA H100**, e sua página oficial de *Capacity Blocks* apresenta preço efetivo de **US$ 31,464/hora** para essa instância em determinadas regiões. Para simular 48 GPUs H100, seriam necessárias 6 instâncias, resultando em custo aproximado de **R$ 690.040,07 por mês** e **R$ 82.804.808,10 em 10 anos**, apenas para capacidade computacional.

16.10. Como referência adicional, a *Google Cloud* informa que a máquina **a3-highgpu-8g** possui **8 GPUs NVIDIA H100**, 208 vCPUs, 1.872 GB de memória, 6.000 GiB de SSD local e até 1.000 Gbps de largura de banda. A página oficial de preços da *Google Cloud* indica valor aproximado de **US$ 88,49/hora** para essa configuração, o que, em cenário equivalente de 48 GPUs, resultaria em aproximadamente **R$ 1.940.682,86 por mês** e **R$ 232.881.943,76 em 10 anos**, apenas em computação.

16.11. Dessa forma, embora nuvem e *colocation* possam aparentar menor desembolso inicial, ambas as alternativas tendem a apresentar custos recorrentes elevados, maior exposição à variação cambial, dependência de disponibilidade de capacidade especializada, risco de aprisionamento tecnológico e ausência de formação de ativo institucional permanente. Em contraposição, a Solução 1 converte o investimento em infraestrutura própria, incorporada ao patrimônio tecnológico do Exército Brasileiro, com possibilidade de uso por múltiplos ciclos de processamento, futuras expansões e novas demandas institucionais.

16.12. A Solução 1 também apresenta vantagem econômica indireta por aproveitar área já existente no DC RF, preservar a governança operacional do ambiente, reduzir custos de interconexão externa, evitar despesas recorrentes de contratação de capacidade de terceiros e permitir maior controle sobre manutenção, expansão, segurança, climatização, energia e monitoramento. Além disso, ao preparar a infraestrutura para evolução tecnológica gradual, inclusive com previsão de suporte futuro a *liquid cooling*, reduz-se o risco de obsolescência prematura e de nova intervenção estrutural em curto prazo.

16.13. Conclui-se, portanto, que a Solução 1 - Expansão da Sala Segura Modular dentro do *Data Center* Coronel Ricardo Franco, contemplando POD de IA e 2 (dois) PODs padrão - é economicamente justificada por apresentar o melhor equilíbrio entre investimento inicial, custo total de propriedade, previsibilidade orçamentária, geração de ativo permanente, redução de dependência externa, soberania tecnológica e capacidade de atendimento continuado às demandas estratégicas de Inteligência Artificial e às demandas convencionais de TIC do Exército Brasileiro.

16.14. **Do Parcelamento da Contratação Decorrente de Aspectos Econômicos:**

16.14.1. Em que pese a solução ser constituída por materiais e serviços distintos julga-se, do ponto de vista econômico, que o parcelamento poderá prejudicar a economia de escala e que não há outras vantagens que justifiquem o parcelamento, principalmente considerando os prejuízos de ordem técnica.

16.14.2. Registra-se que o não parcelamento não tem potencial de prejudicar a competitividade, haja vista que o mercado de TIC é capaz de fornecer soluções de patamar igual ou maior ao que se vislumbra para a solução em estudo.

16.14.3. Adicionalmente verifica-se viável a formação de consórcios para fornecimento da solução, em função do aspecto multidisciplinar dos seus componentes, fator que corrobora com a capacidade do mercado em fornecer a solução como um todo, sem prejuízos à competitividade do certame

17. Contratações Correlatas

17.1. Foram identificadas contratações correlatas realizadas no âmbito do Sistema de Telemática do Exército - SisTEx, as quais guardam relação técnica, operacional ou estratégica com a presente contratação, especialmente por

envolverem padronização de soluções, modernização de ambientes de hospedagem, ampliação de capacidade, segurança da informação, virtualização, *backup*, conectividade e evolução da infraestrutura corporativa de TIC do Exército Brasileiro.

17.2. As contratações correlatas não substituem a presente contratação, pois possuem escopos distintos. Contudo, demonstram a existência de uma estratégia institucional continuada de padronização, modernização, ampliação e segurança da infraestrutura de TIC do SisTEx, da qual a expansão do *Data Center* Coronel Ricardo Franco passa a fazer parte como componente estruturante para hospedagem de sistemas, processamento de dados e sustentação de cargas críticas, inclusive aquelas associadas à Inteligência Artificial e aos novos PODs padrão.

17.3. As principais contratações correlatas identificadas são as seguintes:

Contratação correlata	Órgão/ UASG	Objeto	Correlação com a presente contratação
Adesão ao SRP nº 15/2020 do Ministério da Economia	3º CTA - UASG 160486/ Ministério da Economia - UASG 201057	Aquisição centralizada de licenças VMware para todas as unidades do SisTEx, visando à padronização da solução de virtualização	Relaciona-se à camada de virtualização dos ambientes de hospedagem, que poderá ser suportada pela infraestrutura física ampliada do Data Center
SRP nº 8/2022	CITEx - UASG 160091	Aquisição de Solução de Backup composta por equipamentos, software e serviços para expansão da infraestrutura de armazenamento de backup de todo o SisTEx	Relaciona-se à continuidade operacional, proteção de dados e recuperação de sistemas hospedados nos ambientes corporativos
SRP nº 14/2022	CITEx - UASG 160091	Aquisição de Solução para Evolução do Backbone de Integração — BBI, composta por equipamentos, software e serviços para expansão da infraestrutura de backbone do SisTEx, de abrangência nacional	Relaciona-se à conectividade nacional necessária para acesso, integração e transporte de dados entre os ambientes de hospedagem e as organizações militares
SRP nº 11/2022	7º CTA - UASG 160486	Aquisição de solução de TIC para modernização, padronização e aumento de capacidade dos Ambientes de Hospedagem — AH, composta por equipamentos e software, em atendimento às unidades do SisTEx	Relaciona-se diretamente à modernização dos ambientes de hospedagem, complementando a infraestrutura física e lógica que será ampliada pelo presente projeto
SRP nº 3/2023	7º CTA - UASG 160486	Aquisição de solução de TIC para modernização, padronização e aumento de capacidade dos Ambientes de Hospedagem — AH, composta por equipamentos e software, em atendimento às unidades do SisTEx	Reforça a estratégia de evolução dos ambientes de hospedagem, sendo complementar à ampliação da capacidade física, elétrica, térmica e operacional do Data Center
SRP nº 3/2023	CITEx - UASG 160091	Aquisição de Solução de Segurança de Perímetro e Acesso Padronizado à Internet para todo o Exército Brasileiro, composta por equipamentos, softwares e serviços	Relaciona-se à proteção das bordas de rede e ao acesso seguro à Internet, complementando a segurança lógica dos sistemas hospedados no Data Center

SRP nº 6/2023	CITEx - UASG 160091	Aquisição de Solução de Segurança de Aplicação Web Padronizado para todo o Exército Brasileiro, composta por licenças, softwares e serviços	Relaciona-se à proteção das aplicações web hospedadas nos ambientes corporativos, reforçando a segurança das soluções executadas sobre a infraestrutura do SisTEx

17.4. As contratações acima demonstram que o SisTEx vem adotando modelo de padronização tecnológica em camadas complementares, abrangendo virtualização, *backup*, *backbone*, ambientes de hospedagem, segurança de perímetro e segurança de aplicação. A presente contratação se insere nesse contexto como iniciativa voltada à ampliação da camada física e operacional do *data center*, viabilizando energia, climatização, espaço seguro, monitoramento, *racks*, conectividade passiva, continuidade operacional e capacidade de hospedagem para novas cargas críticas.

17.5. A correlação com as contratações de virtualização decorre da necessidade de sustentar ambientes computacionais padronizados, capazes de hospedar sistemas corporativos e cargas de trabalho de forma segura, resiliente e escalável. A expansão do *Data Center* Coronel Ricardo Franco permitirá que essas camadas lógicas operem sobre infraestrutura física compatível com as demandas atuais e futuras do Exército Brasileiro.

17.6. A correlação com as contratações de *backup* decorre da necessidade de assegurar proteção, retenção, recuperação e continuidade dos dados e sistemas hospedados. A ampliação da infraestrutura do *Data Center* deve ser compatível com políticas de *backup*, replicação, recuperação de desastres e continuidade operacional já estruturadas no âmbito do SisTEx.

17.7. A correlação com a evolução do Backbone de Integração - BBI decorre da necessidade de conectividade nacional, segura e resiliente para acesso aos serviços hospedados nos *Data Centers* Corporativos do Exército. A ampliação do *Data Center* Coronel Ricardo Franco aumenta a capacidade de hospedagem e processamento, enquanto o backbone viabiliza a integração dessas capacidades com as organizações militares e demais pontos da rede corporativa.

17.8. A correlação com as contratações voltadas aos Ambientes de Hospedagem - AH decorre da convergência de finalidade: modernizar, padronizar e ampliar a capacidade de hospedagem de sistemas do Exército. Enquanto os SRP anteriores trataram de equipamentos e *softwares* destinados aos ambientes de hospedagem, a presente contratação trata da infraestrutura crítica necessária para acomodar, energizar, refrigerar, proteger, monitorar e sustentar esses ambientes em condições adequadas de disponibilidade e segurança.

17.9. A correlação com as soluções de segurança de perímetro e de segurança de aplicação *web* decorre da necessidade de proteção em profundidade. A presente contratação reforça a camada física, ambiental e operacional do *data center*, enquanto as contratações correlatas de segurança lógica protegem o tráfego, os acessos, as aplicações e as interações externas dos sistemas hospedados.

17.10. Não se verifica sobreposição indevida de objeto entre a presente contratação e as contratações correlatas identificadas. As aquisições anteriores tratam predominantemente de camadas lógicas, equipamentos de TIC, *softwares*, conectividade, segurança e padronização de ambientes, enquanto esta contratação tem por objeto a expansão da infraestrutura crítica do *data center*, incluindo sala segura, energia, climatização, *racks*, monitoramento, segurança física, combate a incêndio, moving, POD de IA e 2 (dois) PODs padrão.

17.11. As contratações correlatas evidenciam, ainda, que a expansão do *Data Center* Coronel Ricardo Franco é medida coerente com a trajetória institucional de modernização do SisTEx, pois amplia a base física e operacional necessária para sustentar os investimentos já realizados em virtualização, *backup*, backbone, ambientes de hospedagem e segurança.

17.12. Dessa forma, a presente contratação deve ser compreendida como complementar e estruturante em relação às demais iniciativas do SisTEx, contribuindo para consolidar um ecossistema integrado, padronizado, seguro, resiliente e soberano de TIC no âmbito do Exército Brasileiro.

18. Benefícios a serem alcançados com a contratação

18.1. A contratação proporcionará ao 7° CTA, ao SisTEx e ao Exército Brasileiro a ampliação da capacidade institucional de hospedagem, processamento e sustentação de sistemas estratégicos, por meio da expansão do *Data Center* Coronel Ricardo Franco, ambiente próprio, controlado e operado no âmbito do Sistema de Telemática do Exército.

18.2. O principal benefício institucional consiste na criação de capacidade permanente para suportar cargas computacionais críticas, incluindo aplicações de Inteligência Artificial, sistemas corporativos, bancos de dados, plataformas de comando e controle, soluções de apoio à decisão, sistemas administrativos e demais serviços digitais essenciais à Força.

18.3. A solução fortalecerá a soberania dos dados do Exército Brasileiro, ao permitir que informações sensíveis, bases de dados, modelos de IA, artefatos de treinamento, fluxos de processamento, *logs*, metadados e demais ativos digitais estratégicos permaneçam em ambiente próprio, sob controle físico, lógico, administrativo e operacional da Administração.

18.4. A implantação da infraestrutura própria reduz a dependência de soluções externas de mercado, especialmente de provedores de nuvem pública ou ambientes de terceiros, mitigando riscos relacionados à exposição de dados, condicionantes contratuais, restrições tecnológicas, dependência de fornecedor, custos recorrentes variáveis, dificuldade de auditoria e perda de controle sobre a cadeia de custódia da informação.

18.5. A contratação contribuirá para a autonomia tecnológica do Exército Brasileiro, permitindo que a Força disponha de infraestrutura própria para desenvolvimento, treinamento, ajuste, validação e operação de soluções de Inteligência Artificial, sem depender exclusivamente da disponibilidade, das regras comerciais ou da política de segurança de provedores externos.

18.6. A solução permitirá o fortalecimento da governança de TIC no âmbito do Exército, ao concentrar a capacidade de processamento em ambiente institucional, padronizado, monitorado e aderente às diretrizes do SisTEx, facilitando a gestão dos ativos, a rastreabilidade das operações, a aplicação de políticas de segurança e a fiscalização dos recursos empregados.

18.7. A expansão do *Data Center* Coronel Ricardo Franco ampliará a capacidade de atendimento às demandas atuais e futuras do Exército Brasileiro, contemplando tanto o ambiente de alta densidade voltado à Inteligência Artificial quanto a implantação de 2 (dois) PODs padrão, destinados à hospedagem de cargas convencionais de TIC e à absorção de novas demandas operacionais.

18.8. A implantação dos 2 (dois) PODs padrão proporcionará melhor aproveitamento da infraestrutura expandida, permitindo organizar e acomodar servidores e ativos de TIC de menor densidade energética e térmica, sem ocupar indevidamente a capacidade destinada ao processamento intensivo de Inteligência Artificial.

18.9. A contratação permitirá maior disponibilidade dos serviços digitais hospedados no *data center*, uma vez que a solução deverá preservar os atributos de redundância, continuidade operacional e manutenibilidade concorrente associados à certificação Tier III do *Uptime Institute*.

18.10. A solução contribuirá para a continuidade operacional dos sistemas críticos do Exército Brasileiro, reduzindo riscos de indisponibilidade decorrentes de limitações elétricas, térmicas, físicas ou operacionais da infraestrutura atual.

18.11. A ampliação da capacidade elétrica, de climatização, de UPS, de geração de energia, de monitoramento e de segurança física permitirá hospedar equipamentos de maior densidade com maior segurança operacional, reduzindo riscos de sobrecarga, pontos quentes, falhas de energia, indisponibilidade e degradação de desempenho.

18.12. A contratação possibilitará a modernização da infraestrutura crítica do *data center*, incorporando tecnologias compatíveis com ambientes de alta densidade, como climatização de precisão, confinamento térmico, *Rear Door Heat Exchangers*, máquinas *In-Row*, monitoramento ambiental integrado, sensores, controle de acesso, CFTV e sistemas de detecção e combate a incêndio adequados a ambientes de missão crítica.

18.13. A solução criará condições para evolução tecnológica gradual, especialmente no que se refere à futura adoção de *liquid cooling*, permitindo que o Exército acompanhe a evolução dos equipamentos de processamento de IA sem necessidade de nova intervenção estrutural de grande porte em curto prazo.

18.14. O projeto também beneficiará a segurança da informação, ao reforçar o controle de acesso físico, o monitoramento ambiental, a vigilância por CFTV, a detecção precoce de eventos, a proteção contra incêndio e a rastreabilidade de ocorrências no ambiente de *data center*.

18.15. A contratação proporcionará maior proteção aos ativos críticos de TIC, pois a nova sala segura deverá oferecer proteção física compatível com a criticidade dos equipamentos hospedados, incluindo resistência ao fogo, estanqueidade, controle ambiental, segregação física e integração com os sistemas de segurança e monitoramento.

18.16. A solução ampliará a capacidade do Exército de desenvolver e sustentar aplicações de IA em áreas como defesa cibernética, logística, saúde, ensino, vigilância, monitoramento, gestão administrativa, análise de dados, apoio à decisão, comando e controle e demais áreas de interesse estratégico.

18.17. A disponibilidade de infraestrutura própria para IA permitirá reduzir o tempo de processamento de grandes volumes de dados, acelerar ciclos de experimentação, treinamento e inferência de modelos, bem como apoiar projetos institucionais que dependam de processamento massivo e armazenamento de alto desempenho.

18.18. A contratação fortalecerá a capacidade de resposta institucional do Exército Brasileiro, permitindo maior prontidão tecnológica para atender demandas emergentes de processamento, integração de sistemas, análise de informações e suporte a operações administrativas e militares.

18.19. A solução contribuirá para a racionalização de recursos públicos ao transformar o investimento em ativo permanente da Administração, incorporado ao patrimônio tecnológico do Exército Brasileiro, em vez de converter a necessidade em despesa recorrente e dependente de terceiros.

18.20. A expansão do *data center* também permitirá maior previsibilidade orçamentária, pois reduz a exposição a custos variáveis de serviços externos, variação cambial, cobrança por tráfego, armazenamento, processamento sob demanda, suporte gerenciado e custos de saída ou migração.

18.21. A implantação do projeto favorecerá a formação, retenção e aprimoramento de competências internas em operação de infraestrutura crítica, *data center* de alta densidade, climatização especializada, monitoramento, continuidade operacional, segurança física, governança de TIC e sustentação de ambientes voltados à Inteligência Artificial.

18.22. O projeto reforçará o papel estratégico do *Data Center* Coronel Ricardo Franco como infraestrutura central de hospedagem, processamento e sustentação de serviços digitais do Exército Brasileiro, ampliando sua relevância institucional no suporte ao SisTEx, aos sistemas corporativos e às futuras iniciativas de transformação digital da Força.

18.23. A contratação contribuirá para a interoperabilidade e a integração institucional, ao permitir que sistemas corporativos e soluções de IA sejam hospedados em ambiente seguro, de alta disponibilidade e conectado à infraestrutura de comunicações do Exército, favorecendo a integração entre órgãos, comandos, organizações militares e sistemas de interesse da Defesa.

18.24. A solução permitirá mitigar riscos estratégicos associados à insuficiência de capacidade computacional própria, evitando que o Exército Brasileiro fique limitado quanto à implantação de novas soluções digitais, modernização de sistemas, uso de IA e sustentação de cargas críticas.

18.25. A contratação também trará benefícios à gestão de riscos, pois permitirá maior controle sobre disponibilidade, segurança física, energia, climatização, acesso, monitoramento, contingência, manutenção e documentação técnica do ambiente expandido.

18.26. Ao final da implantação, espera-se que o Exército Brasileiro disponha de infraestrutura mais robusta, segura, escalável, resiliente e tecnologicamente atualizada, capaz de sustentar o crescimento das demandas de TIC e de Inteligência Artificial de forma soberana, controlada e alinhada aos interesses estratégicos da Defesa Nacional.

18.27. Dessa forma, os benefícios esperados transcendem a ampliação física do *data center*, alcançando dimensões institucionais, estratégicas, operacionais, tecnológicas e econômicas, com impacto direto na soberania dos dados, na autonomia tecnológica, na continuidade dos serviços digitais, na proteção dos ativos críticos e no fortalecimento da capacidade de transformação digital do Exército Brasileiro.

19. Providências a serem Adotadas

19.1. Considerando as características do objeto e o contexto do 7° CTA julga-se que a solução deverá ser contratada por intermédio de licitação da modalidade Pregão, em sua forma eletrônica, com o critério de julgamento menor preço por grupo, nos termos da Lei nº 14.133, de 1º de abril de 2021.

19.2. Deverá ser prevista a possibilidade de formação de consórcio com exigência de indicação de empresa líder, responsável pela representação perante a Administração, de forma a manter a governança contratual.

> 19.2.1. Justifica-se a admissão de participação de licitantes organizadas em consórcio em função da multiplicidade de especialidades envolvidas na solução, possibilitando, desta feita, a reunião de capacidades técnicas complementares, ao passo que fabricantes, integradores e fornecedores especializados possam contribuir com sua expertise específica.
>
> 19.2.2. A formação do consórcio também é justificada pela vertente da economicidade, pois possibilitará a redução de custos de intermediação, margens sucessivas, retributação e outros custos indiretos decorrentes da concentração artificial de todos os itens em um único fornecedor. Dessa forma vislumbra-se que empresas especializadas pratiquem seus preços próprios para as suas respectivas parcelas do objeto.
>
> 19.2.3. Deverá ser evidenciada no TR a responsabilidade solidária das consorciadas pelos atos praticados em consórcio.

19.3. Deverá ser observado o tratamento da lei de licitações quanto as sociedades cooperativas, admitindo sua participação no certame desde que haja compatibilidade entre seu objeto social, sua forma de organização e a execução do objeto.

> 19.3.1. Tal disposição justifica-se pela intenção de não comprometer, restringir ou frustrar o caráter competitivo do processo licitatório.
>
> 19.3.2. A participação de cooperativas deverá ser condicionado ao atendimento dos requisitos de habilitação jurídica, fiscal, trabalhista, econômico-financeira e técnico-operacional previstos no instrumento convocatório.

19.4. Não será admitida a participação de pessoas físicas no certame, tendo em vista as características e a complexidade do objeto, que exigem estrutura empresarial compatível com a execução da solução, incluindo comprovação de capital social mínimo, disponibilidade de equipe multidisciplinar e corpo técnico especializado, requisitos incompatíveis com a participação de pessoa física, nos termos do parágrafo único do art. 4º da Instrução Normativa SEGES/ME nº 116, de 21 de dezembro de 2021.

> 19.4.1. A restrição decorre da necessidade de assegurar capacidade econômico-financeira, técnica, operacional e organizacional suficiente para execução integrada dos diversos subsistemas da solução, não constituindo limitação arbitrária à competitividade.

19.5. Deverá ser prevista a admissão de subcontratação parcial, limitada a percentual a ser definido no TR, apenas para parcelas acessórias, especializadas ou dependentes de credenciamento técnico específico, sem transferência da responsabilidade integral da contratada.

> 19.5.1. A medida se justifica pela presença de sistemas críticos que podem demandar intervenção de fabricantes ou assistências técnicas credenciadas, notadamente em *nobreaks*, GMGs, *chillers*, climatização de precisão, automação e sistemas especializados.
>
> 19.5.2. A subcontratação não poderá alcançar a parcela principal da obrigação nem comprometer a integração, a padronização, a compatibilidade e a responsabilidade una pela entrega da solução.

19.6. Após o detalhamento do objeto no TR deverão ser formuladas condições de comprovação de Qualificação Técnica a qual é necessária para comprovar que a futura contratada reúne condições para suportar os deveres da contratação, com vistas a reduzir os riscos e garantir o cumprimento das obrigações pertinentes à execução do objeto, em função dos seguintes aspectos de ordem técnica:

19.6.1. A relevância e abrangência do *data center* principal do Exército Brasileiro (DC1-EB), e dos respectivos serviços e aplicações hospedados, no âmbito da Força Terrestre;

19.6.2. A complexidade técnica da expansão da capacidade do *data center* a qual é essencial para suportar o processamento de IA;

19.6.3. A integração de ambientes e sistemas interdependentes os quais são responsáveis pela operação e manutenção do ambiente seguro de dados, preservando a resiliência operacional e continuidade dos serviços críticos; e

19.6.4. O aspecto fundamental quanto a execução correta do objeto, cujo foco refere-se à ampliação da capacidade institucional de hospedagem, processamento e sustentação de sistemas estratégicos, por meio da expansão do *Data Center* Coronel Ricardo Franco, ambiente próprio, controlado e operado no âmbito do Sistema de Telemática do Exército.

20. Disposições Finais

20.1. As informações contidas neste Estudo Técnico Preliminar não são classificadas como sigilosas por não serem consideradas imprescindíveis à segurança da sociedade ou do Estado, nos termos da Lei nº 12.527, de 18 de novembro de 2011.

21. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

21.1. Justificativa da Viabilidade

21.1.1. Considerando:

21.1.1.1. Que este ETP foi demandado de acordo com Despacho Unificado/ Portaria referente ao Documento de Formalização da Demanda (DFD) nº 2/2026, do 7º CTA, o qual atende o escalão superior que demonstra interesse na expansão de *data center*, em atendimento ao DIEx nº 60-E5/CITEx, de 14 de janeiro de 2026;

21.1.1.2. Que o presente estudo foi elaborado em harmonia com o art. 11 da IN SGD/ME nº 94/2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

21.1.1.3. Que, de acordo com as informações levantadas nesse estudo, há conformidade da solução selecionada com as necessidades e os requisitos técnicos necessários à satisfação das necessidades, objeto da contratação;

21.1.1.4. Que a solução atende adequadamente às demandas de negócio formuladas e que os benefícios pretendidos são adequados;

21.1.1.5. Que os motivos que justificam a necessidade de expansão do DC RF, o alinhamento estratégico, as necessidades de negócio e tecnológicas foram fundamentados nesse documento de forma clara, objetiva e detalhada. Os estudos mostraram que a contratação para expansão do DC RF, operado pelo 7º CTA, é viável e necessária; e

21.1.1.6. Que a solução escolhida e indicada neste estudo atende efetivamente o objetivo de expandir a capacidade de hospedagem do *Data Center* Corporativo do Exército Brasileiro em Brasília (*Retrofit* do *Data Center* Ricardo Franco) visando sustentar infraestrutura de TI para suportar IA. Além disso, em seu desenvolvimento, foram agregados fatores e justificativas de projeto que visam a economia de recursos públicos (eficiência e economicidade).

21.1.2. Esta equipe de planejamento, considerando todo o exposto, julga **viável** a contratação da solução escolhida e indicada neste estudo.

22. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

JOSE EDUARDO FRANCA

Coronel - Integrante Requisitante

Assinou eletronicamente em 19/10/2026 às 15:39:11.

ANDERSON ALMEIDA MARQUES

Major - Integrante Técnico

Assinou eletronicamente em 19/10/2026 às 15:30:12.

RODRIGO ROCHA RIBEIRO

Primeiro-Tenente – Integrante Técnico

Assinou eletronicamente em 19/10/2026 às 15:29:19.

LUCAS CAMPOS DA SILVA

Segundo-Tenente - Integrante Técnico

Assinou eletronicamente em 19/10/2026 às 15:26:48.

Despacho: Após análise, na condição de Autoridade Máxima da Área de TIC do 7º CTA e, em atenção ao § 2º do Art. 11 da Instrução Normativa SGD /ME nº 94, de 23 de dezembro de 2022, APROVO o presente ETP.

MATHEUS MOTA PIRES

Major - Autoridade Máxima da Área de TIC

Assinou eletronicamente em 19/10/2026 às 15:37:37.